U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

SEARCH REQUEST FORM Needed on 12/2/98

Requestor's Name: John J. Meyer Serial Number: 08/883636 (152)

Date: 11/30/98 Phone: 308-9046 Art Unit: 2767

Search Topic:
Please write a detailed statement of search topic. Describe specifically as possible the subject matter to be searched. Define any terms that may have a special meaning. Give examples or relevent citations, authors, keywords, etc., if known. For sequences, please attach a copy of the sequence. You may include a copy of the broadest and/or most relevent claim(s).

File Date: 6/26/97

Inventor: Li Gong

Assignee: Sun Microsystems

General Topic: Network Layers (Protocols) and Encryption

Specific Topic: Layer Independent encryption
OR
Communication Protocol independent encryption

Keywords/Phrases: Protocol independent
Layer independent
Secure channel
Java stream
Java Secure Channel

Example: Encrypting a pure data segment with no header (layer dependent) information attached.

STAFF USE ONLY

Date completed: 12/2
Searcher: [illegible]
Terminal time: 25
Elapsed time: 2:00
CPU time:
Total time: 135
Number of Searches: 1
Number of Databases: 45

Search Site
✓ STIC EIC
CM-1
Pre-S

Type of Search
N.A. Sequence
A.A. Sequence
Structure
✓ Bibliographic

Vendors
IG
STN
✓ Dialog
APS
Geninfo
SDC
DARC/Questel
Other

PTO-1590 (9-90)

=> d 1- ti,fd,ab

=> s (java(a)stream?) or (java(a)secur?) or (java(a)channel)

```
       250 JAVA
    251924 STREAM?
         0 JAVA(A)STREAM?
       250 JAVA
    783472 SECUR?
         1 JAVA(A)SECUR?
       250 JAVA
    334753 CHANNEL
         0 JAVA(A)CHANNEL
L10      1 (JAVA(A)STREAM?) OR (JAVA(A)SECUR?) OR (JAVA(A)CHANNEL)
```

=> d l10 ti,ab,fd

FILE 'USPAT' ENTERED AT 14:35:07 ON 25 NOV 1998

```
 **********************************
 *       WELCOME TO THE           *
 *    U.S. PATENT TEXT FILE       *
 **********************************
```

=> query java(a)stream?

L1 QUE JAVA(A)STREAM?

=> query java(a)encrypt?

L2 QUE JAVA(A)ENCRYPT?

=> s l1

```
       256 JAVA
    252345 STREAM?
L3       0 JAVA(A)STREAM?
```

=> s l2

```
       256 JAVA
      5585 ENCRYPT?
L4       0 JAVA(A)ENCRYPT?
```

=> s java(p)(stream?)

```
       256 JAVA
    252345 STREAM?
L5       7 JAVA(P)(STREAM?)
```

=> s java(p)encrypt?

```
       256 JAVA
      5585 ENCRYPT?
L6       5 JAVA(P)ENCRYPT?

=> d 1- ti,fd,ab
=> s java(p)(channel)

       256 JAVA
    335291 CHANNEL
L7       2 JAVA(P)(CHANNEL)


FILE 'USPAT' ENTERED AT 16:26:16 ON 30 NOV 1998

 **********************************
 *       WELCOME TO THE           *
 *    U.S. PATENT TEXT FILE       *
 **********************************

=> query multi-cast? or multicast? or webcast? or broadcast?

      MULTI-CAST?
       (MULTI(W)CAST?)
L1   QUE MULTI-CAST? OR MULTICAST? OR WEBCAST? OR BROADCAST?

=> query network or internet

L2   QUE NETWORK OR INTERNET

=> s l1 and l2

     231228 MULTI
     186693 CAST?
        183 MULTI-CAST?
            (MULTI(W)CAST?)
        882 MULTICAST?
          0 WEBCAST?
      27479 BROADCAST?
     144465 NETWORK
       2423 INTERNET
L3     11553 L1 AND L2

=> s l3 and multi-cast or multicast

     231228 MULTI
     105596 CAST
        154 MULTI-CAST
            (MULTI(W)CAST)
        808 MULTICAST
L4      882 L3 AND MULTI-CAST OR MULTICAST

=> s l3 and( multi-cast or multicast)

     231228 MULTI
     105596 CAST
```

```
       154 MULTI-CAST
           (MULTI(W)CAST)
       808 MULTICAST
L5     855 L3 AND( MULTI-CAST OR MULTICAST)

=> s l5 and (stream?)

    252345 STREAM?
L6     397 L5 AND (STREAM?)

=> s l6 and (protocol or layer)

     40449 PROTOCOL
    533380 LAYER
L7     341 L6 AND (PROTOCOL OR LAYER)

=> d 1-20 ti,fd,ab

FILE 'USPAT' ENTERED AT 17:01:29 ON 30 NOV 1998

 ************************************
 *        WELCOME TO THE            *
 *     U.S. PATENT TEXT FILE        *
 ************************************

=> s (multi-stream or multiple(a)stream)(p)(network or internet)

    231228 MULTI
    223427 STREAM
       111 MULTI-STREAM
           (MULTI(W)STREAM)
    380834 MULTIPLE
    223427 STREAM
    144465 NETWORK
      2423 INTERNET
L1      19 (MULTI-STREAM OR MULTIPLE(A)STREAM)(P)(NETWORK OR INTERNET)

=> d 1- ti,fd,ab
```

Cover Sheet

*** 08/883636***

Prepared for: John Meyer

By : Malinda Garris

Date : December 1, 1998

Attached are your search results. Please review the search and let me know if you would like any other terms/concepts searched. I ran an author search in the patents and retrieved no hits.

My number is 305-0757

Thanks!

Malinda Garris
Electronic Information Center

```
File  15:ABI/INFORM(R) 1971-1998/Dec 01
         (c) 1998 UMI
File   9:Business & Industry(R) Jul 1994-1998/Dec 01
         (c) 1998 Resp. DB Svcs.
File 610:Business Wire 1986-1998/Dec 01
         (c) 1998 Business Wire
File 647:CMP  Computer Fulltext 1988-1998/Nov W2
         (c) 1998 CMP
File 621:IAC New Prod.Annou.(R) 1985-1998/Dec 01
         (c) 1998 Information Access Co
File 674:Computer News Fulltext 1989-1998/Nov W5
         (c) 1998 IDG Communications
File 275:IAC(SM) Computer Database(TM) 1983-1998/Dec 01
         (c) 1998 Info Access Co
File  47:Magazine Database(TM) 1959-1998/Dec 01
         (c) 1998 Information Access Co.
File 636:IAC Newsletter DB(TM) 1987-1998/Dec 01
         (c) 1998 Information Access Co.
File  16:IAC PROMT(R) 1972-1998/Dec 01
         (c) 1998 Information Access Co.
File 148:IAC Trade & Industry Database 1976-1998/Dec 01
         (c) 1998 Info Access Co
File 624:McGraw-Hill Publications 1985-1998/Nov 25
         (c) 1998 McGraw-Hill Co. Inc

Set     Items   Description
S1       9898   (INDEPENDENT? OR SEPARATE?)(N2) (LAYER? OR PROTOCOL?)
S2    1123462   SECURITY? OR ENCRYPTION? OR DECRYPTION? OR CRYPTO?
S3        986   (SECURE()CHANNEL? OR JAVA(N2)STREAM? OR JAVA()SECURE()CHAN-
            NEL?)
S4      29331   (FIRST AND SECOND)(N2)(NODE? OR PROCESS?)
S5      24577   COMMUNICATION?(N)PROTOCOL?
S6         19   ((COMMUNICATION?)(N2)(CHANNEL? OR PROTOCOL?))(N50)(S2(N3)I-
            NDEPENDENT?)
S7          3   S3 AND S1
S8       1822   S1 AND S2
S9        128   S8 AND S5
S10       230   S1(N10)S2
S11         0   S5 (S)S10
S12         7   S5 AND S10
S13        19   S6 AND S2
S14         0   S3AND S4 AND S5
S15         7   S3 AND S4
S16         0   S15 AND (S5 OR S6)
S17       390   (INDEPENDENT?) (N4) (ENCRYPTION? OR CRYPTO? OR DECRYPTION?)
S18         2   S17 (S) ((COMMUNICATION?) (N2) (PROTOCOL? OR CHANNEL?))
S19         0   S17(S)S3
S20         2   S17 AND S3
S21        22   S4(S)(S5 OR S6)
S22         1   S21 AND S1
S23        19   S13 NOT PY=1998
S24        14   RD (unique items)
S25         6   S15 NOT PY=1998
S26         5   RD (unique items)
S27        19   S21 NOT PY=1998
S28        17   RD (unique items)
?
```

7/3,K/1 (Item 1 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

065574
Remtoe access 1999
Prognosticators point to the remote access technologies that will best meet your needs.
Byline: Arielle Emmett
Journal: Network World Page Number: 41
Publication Date: April 06, 1998
Word Count: 2554 Line Count: 234

Text:
...for security (see story, page 43), carriers can offer QoS-type services and carve out **secure channels** to boost performance, she says.
"We see ISPs charging higher fees per port when they...encryption and authentication mechanisms, meaning the ISP and its customers have to address those issues **separately** .
Another **protocol** , IP Security (IPSec), is intended to overcome that limitation by offering X.509 digital certificate...

7/3,K/2 (Item 1 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

02932688
NETSCAPE: Netscape announces Secure Courier -- A digital envelope for securing Internet transactions
M2 Presswire Oct 11, 1995
WORD COUNT: 941
PUBLISHER: M2 Communications

... PC to the financial institution. In addition, Secure Courier enables consumer authentication for merchants. While **secure channel** protocols such as SSL encrypt data passing along the network between a client system and...

... people already have SSL-enabled products, which have been available since December 1994. SSLis application **protocol** - **independent** and provides encryption, which creates a secured channel to prevent others from tapping into the...

7/3,K/3 (Item 1 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

07995389 SUPPLIER NUMBER: 17277850 (USE FORMAT 7 OR 9 FOR FULL TEXT)
NETSCAPE ANNOUNCES SECURE COURIER - A DIGITAL ENVELOPE FOR SECURING FINANCIAL TRANSACTIONS ON THE INTERNET
PR Newswire, p718LA031
July 18, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 793 LINE COUNT: 00087

... PC to the financial institution. In addition, Secure Courier enables consumer authentication for merchants. While **secure channel** protocols such as SSL encrypt data passing along the network between a client system and...

...already have SSL-enabled products, which have been available since December 1994. SSL is application **protocol** - **independent** and provides encryption, which creates a secured channel to prevent others from tapping into the...

12/3,K/1 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01075551 CMP ACCESSION NUMBER: EET19951215S0027
Net looks for secure feeling
Margaret Ryan
ELECTRONIC ENGINEERING TIMES, 1995, n 880, PG54
PUBLICATION DATE: 951215
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Best 1995 Technologies: World Wide Web
WORD COUNT: 1191

... The recipient then unscrambles the message with the secret key. Netscape is also working on **separate security protocols** that are application-specific-for instance, Secure Courier Transaction, co-developed with Mastercard. The protocol...

...and Secure Hypertext Transfer Protocol (S-HTTP), a security-enhanced version of HTTP, the internal **communications protocol** of the World Wide Web. With them, it can communicate with all types of secure...

12/3,K/2 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

00516203 CMP ACCESSION NUMBER: NWC19920601S0354
What Are the Standards for Interoperable LAN Security
Dan Minoli
NETWORK COMPUTING, 1992, n 306 , 148
PUBLICATION DATE: 920601
JOURNAL CODE: NWC LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Workshops
WORD COUNT: 1576

... implementations to specify compliance to SILS Secure Data Exchange, SILS Key Management and SILS System/**Security** Management **independently** . The **protocols** must support a transparent implementation for devices that currently exist on the network. That is...

...of the SILS model. The user stacks shown in the diagram are the existing network **communication protocols** before SILS is implemented. These stacks request security services from SDE. In turn, the SDE...

12/3,K/3 (Item 1 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)

01251285 SUPPLIER NUMBER: 06284720 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Modems tackle real work.
Powell, Dave
Telecommunication Products & Technology, v6, n2, p47(5)
Feb, 1988
ISSN: 0746-6072 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2758 LINE COUNT: 00227

... offers an EC (Encryption Card) option for $1250, which is based on the DES (Data **Encryption** STandard) algorithm approved by the National Bureua of Standards. **Protocol -independent** in point-to-point or multipoint networks, the option encrypts using a randomly generated 64... Another nagging problem for network managers is supporting a growing variety of vendor equipment and **communications protocols** . To some

extent, Bell and CCITT standards have been a saving grace. But, unfortuantely, high...

12/3,K/4 (Item 2 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)

01242845 SUPPLIER NUMBER: 06536751 (USE FORMAT 7 OR 9 FOR FULL TEXT)
OS-2 LAN Manager provides a platform for server-based network applications.
Kessler, Alan
Microsoft Systems Journal, v3, n2, p29(10)
March, 1988
ISSN: 0889-9932 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5004 LINE COUNT: 00417

... garner a large market share. However, NetBIOS requires the application developer to understand a detailed **communication protocol** at very low levels in the system, therefore making NetBIOS applications difficult to develop. Also...

...system software product called OS/2 LAN Server, which also is hosted by OS/2.

Protocol -Independent

Applications written to take advantage of the **security** , network management, or any other LAN Manager feature are portable to many different network environments...

12/3,K/5 (Item 1 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

05893810
Net looks for secure feeling
Issues new encryption software after discovering flaw
Electronic Engineering Times Dec 15, 1995 p. 54
ISSN: 0192-1541
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 1193

...The recipient then unscrambles the message with the secret key.

Netscape is also working on **separate security protocols** that are application-specific-for instance, Secure Courier Transaction, co-developed with Mastercard. The protocol...

...and Secure Hypertext Transfer Protocol (S-HTTP), a security-enhanced version of HTTP, the internal **communications protocol** of the World Wide Web. With them, it can communicate

12/3,K/6 (Item 2 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

03868111
What Are the Standards for Interoperable LAN Security?
Network Computing June, 1992 p. 148
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 1524

...implementations to specify compliance to SILS Secure Data Exchange, SILS Key Management and SILS System/**Security** Management **independently** . The **protocols** must support a transparent implementation for devices that currently exist on the network. That is...

...of the SILS model. The user stacks shown in the diagram are the existing network **communication protocols** before SILS is implemented. These stacks request security services from SDE. In turn, the SDE...

12/3,K/7 (Item 1 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

08379132 SUPPLIER NUMBER: 17990694 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Net looks for secure feeling. (Best 1995 Technologies: World Wide Web)(includes related article on Industry.Net Online Marketplace) (Technology Information)
Ryan, Margaret
Electronic Engineering Times, n880, p54(2)
Dec 15, 1995
ISSN: 0192-1541 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1300 LINE COUNT: 00109

... The recipient then unscrambles the message with the secret key.
Netscape is also working on **separate security protocols** that are application-specific-for instance, Secure Courier Transaction, co-developed with Mastercard. The protocol...

...and Secure Hypertext Transfer Protocol (S-HTTP), a security-enhanced version of HTTP, the internal **communications protocol** of the World Wide Web. With them, it can communicate with all types of secure...

18/3,K/1 (Item 1 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

01002527 53162572

RSA Provides Single Source for Java Security.

PR Newswire
DATELINE: PRNewswire, New SSL and Enhanced Crypto Components Give Developers Complete Package For Java Security Needs SAN MATEO, Calif., Nov. 3 Nov 3, 1998 WORD COUNT: 1008

...session-based encryption and authentication. SSL is a general-purpose protocol, and provides a secure **communications channel** between two points, server authentication, and, optionally, client authentication. As a result, it prevents eavesdropping...

...communications within their applications. Users of SSL include business, government and services development organizations and **independent** software vendors (ISVs).
BSAFE **Crypto** -J
RSA's BSAFE Crypto-J 2.0 builds on the success of its predecessor...

18/3,K/2 (Item 2 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00722368 00722804

SPYRUS and Terisa Systems Announce Strategic Partnership to Combine Cryptographic Toolkits, Protocols, and Applications; Cryptography, protocol, and application solutions are integrated to bring the security benefits of hardware cryptography to multiple protocols.

Business Wire
DATELINE: SAN FRANCISCO Jan 27, 1997 WORD COUNT: 1106

...Secure HTTP is an interoperable extension of the World Wide Web's existing HyperText Transfer **Protocol** that provides **communication** and transaction security for WWW clients and servers. SSL is a transport

level security mechanism...

...provider of high-assurance hardware
cryptographic products that are Algorithm Agile(tm) and form factor
independent . SPYRUS' products provide **encryption** , digital signature,
access control, and metering solutions for Corporate IS,
WWW/Internet and Intranet Applications...

20/3,K/1 (Item 1 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

02932688
NETSCAPE: Netscape announces Secure Courier -- A digital envelope for securing Internet transactions
M2 Presswire Oct 11, 1995
WORD COUNT: 941
PUBLISHER: M2 Communications

... PC to the financial institution. In addition, Secure Courier enables consumer authentication for merchants. While **secure channel** protocols such as SSL encrypt data passing along the network between a client system and...

... already have SSL-enabled products, which have been available since December 1994. SSLis application protocol- **independent** and provides **encryption** , which creates a secured channel to prevent others from tapping into the network; authentication, which...

20/3,K/2 (Item 1 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

07995389 SUPPLIER NUMBER: 17277850 (USE FORMAT 7 OR 9 FOR FULL TEXT)
NETSCAPE ANNOUNCES SECURE COURIER - A DIGITAL ENVELOPE FOR SECURING FINANCIAL TRANSACTIONS ON THE INTERNET
PR Newswire, p718LA031
July 18, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 793 LINE COUNT: 00087

... PC to the financial institution. In addition, Secure Courier enables consumer authentication for merchants. While **secure channel** protocols such as SSL encrypt data passing along the network between a client system and...

...have SSL-enabled products, which have been available since December 1994. SSL is application protocol- **independent** and provides **encryption** , which creates a secured channel to prevent others from tapping into the network; authentication, which...

22/3,K/1 (Item 1 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00545674 00545674

SCSI CONNECTIVITY LIMITATIONS SOLVED WITH NEW, HIGH SPEED ARCHITECTURE FROM VICOM SYSTEMS

PR Newswire
DATELINE: LAS VEGAS Nov 13, 1995 WORD COUNT: 668

...using industry standard SCSI or SSA
interfaces. With multiple simultaneous transmission rates of
640Mbits per **second** , increased **node** - to-node distances and unlimited

devices per channel, SLIC finally enables the promised benefits of...

...SCSI and SSA products. "We expect a number of SLIC implementations will be as an **independent communications protocol** to take advantage of the 640Mbit per second transfer rate and its support of simultaneous...

...high performance communications environments independent of LANs, WANs or other networks and is the only **communications protocol** that supports simultaneous transmissions. SLIC incorporates advanced SCSI features such as command processing, tagged queuing...

24/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01520486 01-71474

Standards promise safe, secure data transmission
Harler, Curt
Managing Office Technology v42n5 PP: 18 May 1997
ISSN: 1070-4051 JRNL CODE: MOP
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 1402.02
WORD COUNT: 608

ABSTRACT: In networking, PICA (Platform-Independent **Cryptography** API) is an emerging standard that will let businesses send data securely over wide area...

... or the Internet. The announcement that Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA Data **Security** , and Silicon Graphics will all support PICA as a **cryptography** API should move data **security** ahead by leaps and bounds. Driving **cryptography** are 4 business needs: 1. confidentiality, 2. integrity, 3. authentication, 4. non-repudiation or proof...
...TEXT: are cute critters which zip around boulders and charm climbers. In networking, PICA (Platform-Independent **Cryptography** API) is an emerging standard that will let businesses send data securely over wide area...

...or the Internet.

The announcement that Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA Data **Security** , and Silicon Graphics will all support PICA as a **cryptography** API should move data **security** ahead by leaps and bounds. PICA addresses interoperability problems that arise as **crypto** technology moves into the mainstream software products of competing vendors.

Jim Bidzos, president of RSA...

...combine the best of all in an open standard.

PICA will build bridges between differing **crypto** approaches to simplify the way different platforms use **cryptography** . It will let developers introduce open, cross-platform, application-**independent security** the same way that they introduce features like graphics, **communications** and networking **protocols** .
Kathy Kincaid, director of **security** programs for IBM, says PICA allows adding **security** features like SSL (**security** socket layer) or DES (data **encryption** standard) to a host of applications, regardless of operating platform. "It will inspire confidence in...

...securely, whether for E-mail, EDI or electronic commerce," she says.

Four business needs drive **cryptography** : confidentiality; integrity, knowing the data was not changed in shipment; authentication, identifying both parties; and non-repudiation or proof of transaction. "PICA will do for **security** what HTML did for the Web," predicts Mike Homer, vice

president of Netscape Communications, Mountain View, CA. Their client and server **security** infrastructure is built on Intel's CDSA (common data **security** architecture), another building block for PICA.

Firms whose Internet and MIS plans are based on...

... Our Novell Directory Services (NDS) represents the world's largest commercial use of public key **cryptography** and is available on multiple platforms. PICA will make it easier to provide secure solutions built on directory services."
Microsoft is notable by its absence from PICA. Its **security** for Internet technologies can be found on its Internet **Security** Framework resources at www.microsoft.com/workshop/ prog/ **security** /. Microsoft promotes Code Signing Technology to reduce the risk of malicious code by identifying who ...

...with. Microsoft's implementation of code signing is called Authenticode. Microsoft has an enhanced Java **security** model in Internet Explorer 4.0 to address applets that may work outside of Java. Microsoft is partnering with third-party vendors like Cisco by joining the Enterprise **Security** Alliance to develop standard **security** across networked clients, servers and infrastructure.

Security products have one drawback: things get lost. How does a business recover a **crypto** key if it is destroyed? The Key Recovery Alliance --supported by Apple, Atalla, DEC, Groupe...

... available to anyone. The key recovery process will support all existing key distribution schemes and **encryption** algorithms, Kincaid says.

Author Affiliation:
Curt Harler is a freelance technology writer and frequent contributor...

DESCRIPTORS: Data **encryption** ; ...

...Computer **security** ;

24/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01163984 98-13379
Net transaction security: **A state of mind**
Kellner, Mark A
CommunicationsWeek n597 PP: IA7, IA9 Feb 19, 1996
ISSN: 0746-8121 JRNL CODE: CWE
AVAILABILITY: Photocopy available from ABI/INFORM

Net transaction security: **A state of mind**

...ABSTRACT: Web sites, there are several things to consider. One is the selection of a transport **protocol** : Private **Communication** Technology, Secure Sockets Layer or Secure-HyperText Transfer Protocol. Another is deciding whether to bypass a transport protocol for an **independent** **security** system, for example licensing RSA Data **Security** Inc.'s data **security** algorithms directly. For small mail-order companies, there is even a script they can add...
COMPANY NAMES:
RSA Data **Security** Inc

DESCRIPTORS: Computer **security** ; ...

...Data **encryption**

24/3,K/3 (Item 1 from file: 610)

0634818 BW0556

RSA DATA SECURITY : Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Building Upon RSA's PKCS Standards Process and Technology Submissions from Industry

October 17, 1996

Byline: Business Editors/Computer Writers

RSA DATA SECURITY : Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Building Upon RSA's PKCS Standards Process and Technology Submissions from Industry

...Silicon Graphics jointly announced their support for an effort code-named PICA, or "Platform-Independent **Cryptography** API."

PICA(tm) builds on RSA's widely-adopted Public Key **Cryptography** Standards (PKCS) process and technology submissions from several companies.

The PICA alliance has been formed primarily to address potential interoperability problems that may arise as **cryptographic** technology moves into the mainstream software products of competing vendors. With open development meetings scheduled for later on this year, PICA vendors will attempt to "build bridges" between their differing **crypto** approaches, and will look for ways to simplify the way developers use **cryptography** on different platforms.

The PICA specification will be designed to allow developers to introduce open, cross-platform, application **independent security** in the same way that they introduce other features like graphics, **communications** , and networking **protocols** . PICA should enable developers to add **security** features such as SSL, DES, and smartcards to electronic commerce, banking, EDI and other applications...

...PICA will also be designed to make the task of developing differing domestic and exportable **security** requirements much easier.

Jim Bidzos, RSA President, said, "The original PKCS group, with members including...

...Graphics, Sun and many others, has been a place where competitors can work together on **crypto** specifications since its formation in 1991.

"It is anticipated that the new PICA efforts will...

...The industry-wide effort is an important step towards simplifying the way developers work with **cryptography** ," he continued "Once a niche application, sophisticated **cryptography** is making its way into even the seemingly most pedestrian Internet applications -- and **crypto** is an important component in hot emerging segments such as electronic commerce, Internet EDI and electronic cash."

"This is an exciting time for **cryptography** . The PICA effort will better enable IBM's SecureWay **cryptographic** infrastructure to provide a less complex, more modular way for developers to build applications which make the Internet safe for business," said Kathy Kincaid, Director of I/T **Security** Programs for IBM.

"This will do for **security** what HTML did for the Web," said Mike Homer, VP Marketing for Netscape. "Netscape is happy to announce that our client and server **security** infrastructure is built on Intel's CDSA, a potential building block for PICA. We selected...

...support."

"The PICA alliance will make it easier for developers to provide customers with important **security** features such as privacy of

communications, authentication of identity, and viable electronic commerce in a...

...are encouraged to see the industry working with the PICA-PKCS process to establish Internet **security** specifications to offer an open standard, and we look forward to participating in the process to lead its impact on Java," said Li Gong, **security** architect at JavaSoft, a business unit of Sun Microsystems, Inc.

"Our goal is to integrate strong **security** into all applications, ranging from commercial off-the-shelf to custom legacy applications," said Brad...

...Networks. "Towards that end, Nortel will be contributing APIs developed for the Entrust family of **encryption** and key management products, as well as our experience gained with real world solutions, to...

...WebFORCE Group Marketing Manager at Silicon Graphics, said "the recent proliferation of specifications in the **cryptography** arena has not been beneficial to our WebFORCE Internet Server customers or to the industry...

...Our Novell Directory Services (NDS) represents the world's largest commercial use of public key **cryptography** and is available on multiple platforms. PICAA will make it easier for developers to provide...

...provide to our customers," said Don Rothwell, vice president and director of Motorola's Information **Security** Operations. "PICA will allow exciting, new applications to reach the market more quickly than previously possible."

About RSA

RSA Data **Security** , Inc., a wholly owned subsidiary of **Security** Dynamics Technologies, Inc. (NASDAQ: SDTI), is the world's brand name for **cryptography** , with more than 75 million copies of RSA **encryption** and authentication technologies installed and in use worldwide.

RSA technologies are part of existing and...

...develops and markets platform-independent developer's kits and end-user products and provides comprehensive **cryptographic** consulting services. Founded in 1982 by the inventors of the RSA Public Key **Cryptosystem** , the company is headquartered in Redwood City, Calif.

About Apple

Apple Computer, Inc., a recognized...

...http://www.apple.com

About IBM

IBM's SecureWay brand is a comprehensive portfolio of **security** offerings. Whether addressing a specific requirement or creating a total ...networks. Additional information can be found on our SecureWay homepage at http://www.ibm.com **security** .

About JavaSoft

JavaSoft, headquartered in Cupertino, CA, is an operating company of Sun Microsystems Inc...

...and systems for secure communications, Nortel has built a team of world-leading experts in **cryptography** , **security** architecture and international standards.

Nortel's Enterprise Networks group provides custom-designed enterprise networks for...

24/3,K/4 (Item 1 from file: 647)

01082096 CMP ACCESSION NUMBER: CWK19960219S0006

Beyond Technology, What Online Companies Can Do To Reassure Customers - Net transaction security: **A state of mind** (Web Commerce)

Mark A. Kellner

COMMUNICATIONSWEEK, 1996, n 597, PGIA7
PUBLICATION DATE: 960219
JOURNAL CODE: CWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Interactive Age
WORD COUNT: 977

Beyond Technology, What Online Companies Can Do To Reassure Customers - Net transaction security: **A state of mind**

... Web sites, there are several things to consider. One is the selection of a transport **protocol** : Private **Communication** Technology, Secure Sockets Layer or Secure-HyperText Transfer Protocol (see sidebar). Another is deciding whether to bypass a transport protocol for an **independent security** system, say, licensing RSA Data **Security** Inc.'s data **security** algorithms directly.

For smaller businesses-for example, mail-order companies dwarfed by the catalog operations...

...be used to process the order.

At the same time, advocates and marketers of data-**security** products assert it is important to look beyond a given software code and move into a **security** consciousness. Unless businesses are aware of the various possibilities for computer-related crimes, more than...

...Stewart, chief technology officer at back-office software provider Open Market Inc., in Cambridge, Mass. "**Encryption** is a tool that is trying to help you do those things, but it's...

...less-than- honest employees at a given merchant, Stewart said.

But there is a chance **security** could be breached before the transaction even is secured, he added, so companies should be...

...about this kind of thing leads us not just to developing the current round of **encryption** , Stewart said, but toward other options, including smart cards, which he predicted will come online...

...First you have a policy, then you have access control, then you have stuff like **encryption** , then you've also got to have a feedback loop, such as audit trails and...

...to software developer David Bodley at South Florida Mall in Miami, is to pinpoint where **security** breaches are likely to occur. He maintained that hacking individual messages is not very profitable...

...marketing at eShop Inc. , an online shopping service based in San Mateo, Calif., settling the **security** question didn't lie in which **security** algorithm to use. Using both the Internet and X.25 dial-up services, eShop developed...

...independently to provide access and process transactions.

Rather than settling on one algorithm to ensure **security** , eShop instead licensed the Toolkit for Interoperable Privacy-Enhanced Messaging from RSA Data **Security** , in Redwood City, Calif. By encrypting messages, Weinstein said, eShop is able to offer a guarantee of **security** to its customers. "No matter how you access us, you're guaranteed secure transactions. If...

...ll reimburse you. We tackled the perception issue straight on." (See story, page IA6.)

How **security** is perceived is more important than the specific technology, Weinstein added.

"Our personal focus is...

...Agreeing with Bodley and Stewart, Weinstein said the transaction isn't the only area of **security** in which businesses should concentrate.
"It's important that people use their heads when dealing...

24/3,K/5 (Item 2 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01035863 CMP ACCESSION NUMBER: OST19941114S0075
A Web Conference That Almost Anyone Can Enjoy (Shrink Rap)
Jason Levitt
OPEN SYSTEMS TODAY, 1994, n 163, PG81
PUBLICATION DATE: 941114
JOURNAL CODE: OST LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: OST Labs
WORD COUNT: 716

... One paper, ``The DCE Web Project,'' is OSF's attempt to offer a secure, flexible **communications channel** for Web usage based on its DCE (Distributed Computing Environment) technology. At the show, OSF...

...sent over DCE RPCs (remote procedure calls). In order to take full advantage of the **security** and location- **independent** naming features of the DCE Web project, you have to use OSF's modified Web...

...access the DCE Web environment through a gateway, but can't take advantage of the **security** and naming features. Surf the OSF Research Institute's home page at http://riwww.osf...

24/3,K/6 (Item 1 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)

02001404 SUPPLIER NUMBER: 18848675 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Internet security: **Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics announce PICA** crypto-**alliance; building upon RSA's RKCS standards process and technology submission from industry. (Platform-Independent** Cryptography **API, RSA Data** Security's **Public Key** Cryptography **Standards) (Company Business and Marketing)**
EDGE: Work-Group Computing Report, v7, p18(1)
Oct 28, 1996
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1547 LINE COUNT: 00139

Internet security: **Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics announce PICA** crypto-**alliance; building upon RSA's RKCS standards process and technology submission from industry. (Platform-Independent** Cryptography **API, RSA Data** Security's **Public Key** Cryptography **Standards) (Company Business and Marketing)**

TEXT:
...Silicon Graphics jointly announced their support for an effort code-named PICA, or "Platform-Independent **Cryptography** API."
PICA builds on RSA's widely-adopted Public Key **Cryptography** Standards (PKCS) process and technology submissions from several companies.
The PICA alliance has been formed primarily to address potential interoperability problems that may arise as **cryptographic** technology moves into the mainstream software products of competing vendors. With open development meetings scheduled for later on this year, PICA vendors will attempt to "build bridges" between their differing **crypto** approaches, and will look for ways to simplify the way developers use **cryptography** on different platforms.
The PICA specification will be designed to allow developers to introduce open, cross-platform, application **independent security** in the

same way that they introduce other features like graphics, **communications** , and networking **protocols** . PICA should enable developers to add **security** features such as SSL, DES, and smartcards to electronic commerce, banking, EDI and other applications...

...PICA will also be designed to make the task of developing differing domestic and exportable **security** requirements much easier.

Jim Bidzos, RSA President, said, "The original PKCS group, with members including...

...Graphics, Sun and many others, has been a place where competitors can work together on **crypto** specifications since its formation in 1991.

"It is anticipated that the new PICA efforts will...

...The industry-wide effort is an important step towards simplifying the way developers work with **cryptography** ," he continued "Once a niche application, sophisticated **cryptography** is making its way into even the seemingly most pedestrian Internet applications -- and **crypto** is an important component in hot emerging segments such as electronic commerce, Internet EDI and electronic cash."

"This is an exciting time for **cryptography** . The PICA effort will better enable IBM's SecureWay **cryptographic** infrastructure to provide a less complex, more modular way for developers to build applications which make the Internet safe for business," said Kathy Kincaid, Director of I/T **Security** Programs for IBM.

"This will do for **security** what HTML did for the Web," said Mike Homer, VP Marketing for Netscape. "Netscape is happy to announce that our client and server **security** infrastructure is built on Intel's CDSA, a potential building block for PICA. We selected...

...support."

"The PICA alliance will make it easier for developers to provide customers with important **security** features such as privacy of communications, authentication of identity, and viable electronic commerce in a...

...are encouraged to see the industry working with the PICA-PKCS process to establish Internet **security** specifications to offer an open standard, and we look forward to participating in the process to lead its impact on Java," said Li Gong, **security** architect at JavaSoft, a business unit of Sun Microsystems, Inc.

"Our goal is to integrate strong **security** into all applications, ranging from commercial off-the-shelf to custom legacy applications," said Brad...

...Networks. "Towards that end, Nortel will be contributing APIs developed for the Entrust family of **encryption** and key management products, as well as our experience gained with real world solutions, to...

...WebFORCE Group Marketing Manager at Silicon Graphics, said "the recent proliferation of specifications in the **cryptography** arena has not been beneficial to our WebFORCE Internet Server customers or to the industry...

...Our Novell Directory Services (NDS) represents the world's largest commercial use of public key **cryptography** and is available on multiple platforms. PICAA will make it easier for developers to provide...
...provide to our customers," said Don Rothwell, vice president and director of Motorola's Information **Security** Operations. "PICA will allow exciting, new applications to reach the market more quickly than previously possible."

RSA Data **Security** , Inc., a wholly owned subsidiary of **Security** Dynamics Technologies, Inc., is the world's brand name for **cryptography** , with more than 75 million copies of RSA **encryption** and authentication technologies installed and in use worldwide.

RSA technologies are part of existing and...

...develops and markets platform-independent developer's kits and end-user

products and provides comprehensive **cryptographic** consulting services. Founded in 1982 by the inventors of the RSA Public Key **Cryptosystem** , the company is headquartered in Redwood City, Calif.
Apple Computer, Inc., a recognized innovator in...

...Wide Web: http://www.apple.com
IBM's SecureWay brand is a comprehensive portfolio of **security** offerings. Whether addressing a specific requirement or creating a total end-to-end solution, IBM http://www.ibm.com/**security** .
JavaSoft, headquartered in Cupertino, CA, is an operating company of Sun Microsystems Inc. The company...
...and systems for secure communications, Nortel has built a team of world-leading experts in **cryptography** , **security** architecture and international standards.
Nortel's Enterprise Networks group provides custom-designed enterprise networks for...

...COMPANY NAMES: RSA Data **Security** Inc...
...DESCRIPTORS: **Encryption** ; ...

...Data **Security** Issue

24/3,K/7 (Item 2 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)
(c) 1998 Info Access Co. All rts. reserv.

01904743 SUPPLIER NUMBER: 18015574 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Keeping tabs on standards. (PC Week Netweek) (Brief Article) (Editorial)
Bridges, Linda
PC Week, v13, n7, pN3(1)
Feb 19, 1996
DOCUMENT TYPE: Brief Article Editorial ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1311 LINE COUNT: 00120

... to calculate the most efficient path to other routers over the Internet. Version 2 adds **Cryptographic** authentication, allowing any "Keyed Message Digest" algorithm to be used.
RIP Version II: Routing Information...

...handle secure payment with bank cards over nonsecure data transports such as the Internet.
Internet **Security** Standards at a Glance
PCT: Private **Communication** Technology **Protocol** . PCT is designed to provide privacy between two communicating applications (a client and a server...
...TCP) for data transmission and reception.
SHTTP: Secure Hypertext Transport Protocol. Extension of HTTP providing **independently** applicable **security** services for transaction confidentiality, authenticity/integrity, and non-repudiability of origin.
SSL: Secure Sockets Layer...

24/3,K/8 (Item 1 from file: 47)
DIALOG(R)File 47:Magazine Database(TM)
(c) 1998 Information Access Co. All rts. reserv.

04787007 SUPPLIER NUMBER: 19600815 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Network connectivity gains momentum. (includes related article on data security standards) (Cover Story)
Romei, Lura K.; Harler, Curt
Managing Office Technology, v42, n5, p16(3)
May, 1997
DOCUMENT TYPE: Cover Story ISSN: 1070-4051 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2394 LINE COUNT: 00198

Network connectivity gains momentum. (includes related article on data security standards) (Cover Story)

... each user thinking that his or her application is mission-critical, and suddenly reliability and **security** loom large on the importance scale. What's more, all the users need to be...ISDN association, of which it is a founding member) to develop ISDN technology for home **security** systems. With current home **security** systems, if someone cuts a telephone line, there is no way for **security** professionals to know if a home has been invaded. By using an ISDN D-channel that constantly polls for data, **security** companies will have the ability to know immediately when a phone line is cut.

ISDN...

...are cute critters which zip around boulders and charm climbers. In networking, PICA (Platform-Independent **Cryptography** API) is an emerging standard that will let businesses send data securely over wide area...

...or the Internet.

The announcement that Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA Data **Security** , and Silicon Graphics will all support PICA as a **cryptography** API should move data **security** ahead by leaps and bounds. PICA addresses inter-operability problems that arise as crypro technology...

...combine the best of all in an open standard.

PICA will build bridges between differing **crypto** approaches to simplify the way different platforms use **cryptography** . It will let developers introduce open, cross-platform, application-**independent security** the same way that they introduce features like graphics, **communications** and networking **protocols** .

Kathy Kincaid, director of **security** programs for IBM, says PICA allows adding **security** features like SSL (**security** socket layer) or DES (data **encryption** standard) to a host of applications, regardless of operating platform. "It will inspire confidence in...

...securely, whether for E-mail, EDI or electronic commerce," she says.

Four business needs drive **cryptography** : confidentiality; integrity, knowing the data was not changed in shipment; authentication, identifying both parties; and non-repudiation or proof of transaction. "PICA will do for **security** what HTML did for the Web," predicts Mike Homer, vice president of Netscape Communications, Mountain View, CA. Their client and server **security** infrastructure is built on Intel's CDSA (common data **security** architecture), another building block for PICA.

Firms whose Internet and MIS plans are based on...

...Our Novell Directory Services (NDS) represents the world's largest commercial use of public key **cryptography** and is available on multiple platforms. PICA will make it easier to provide secure solutions built on directory services."

Microsoft is notable by its absence from PICA. Its **security** for Internet technologies can be found on its Internet **Security** Framework resources at www.microsoft.com/workshop/prog/**security** /. Microsoft promotes Code Signing Technology to reduce the risk of malicious code by identifying who...

...with. Microsoft's implementation of code signing is called Authenticode. Microsoft has an enhanced Java **security** model in Internet Explorer 4.0 to address applets that may work outside of Java. Microsoft is partnering with third-party vendors like Cisco by joining the Enterprise **Security** Alliance to develop standard **security** across networked clients, servers and infrastructure.

Security products have one drawback: things get lost. How does a business recover a crypro key...

...available to anyone. The key recovery process will support all existing key distribution schemes and **encryption** algorithms, Kincaid says.

Curt Harler is a freelance technology writer and frequent contributor

to MANAGING...

24/3,K/9 (Item 1 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

03396885
Internet Security : Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Building Upon RSA's PKCS Standards Process and Technology Submissions from Industry
Edge: Work-Group Computing Report Oct 28, 1996
WORD COUNT: 1447
PUBLISHER: EDGE Publishing

Internet Security : Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Building Upon RSA's PKCS Standards Process and Technology Submissions from Industry

... Silicon Graphics jointly announced their support for an effort code-named PICA, or "Platform-Independent **Cryptography** API."

PICA builds on RSA's widely-adopted Public Key **Cryptography** Standards (PKCS) process and technology submissions from several companies.

The PICA alliance has been formed primarily to address potential interoperability problems that may arise as **cryptographic** technology moves into the mainstream software products of competing vendors. With open development meetings scheduled for later on this year, PICA vendors will attempt to "build bridges" between their differing **crypto** approaches, and will look for ways to simplify the way developers use **cryptography** on different platforms.

The PICA specification will be designed to allow developers to introduce open, cross-platform, application **independent security** in the same way that they introduce other features like graphics, **communications** , and networking **protocols** . PICA should enable developers to add **security** features such as SSL, DES, and smartcards to electronic commerce, banking, EDI and other applications...

... PICA will also be designed to make the task of developing differing domestic and exportable **security** requirements much easier.

Jim Bidzos, RSA President, said, "The original PKCS group, with members including...

... Graphics, Sun and many others, has been a place where competitors can work together on **crypto** specifications since its formation in 1991.
"It is anticipated that the new PICA efforts will...

... The industry-wide effort is an important step towards simplifying the way developers work with **cryptography** ," he continued "Once a niche application, sophisticated **cryptography** is making its way into even the seemingly most pedestrian Internet applications -- and **crypto** is an important component in hot emerging segments such as electronic commerce, Internet EDI and electronic cash."

"This is an exciting time for **cryptography** . The PICA effort will better enable IBM's SecureWay **cryptographic** infrastructure to provide a less complex, more modular way for developers to build applications which make the Internet safe for business," said Kathy Kincaid, Director of I/T **Security** Programs for IBM.

"This will do for **security** what HTML did for the Web," said Mike Homer, VP Marketing for Netscape. "Netscape is happy to announce that our client

and server **security** infrastructure is built on Intel's CDSA, a potential building block for PICA. We selected...

...support."
"The PICA alliance will make it easier for developers to provide customers with important **security** features such as privacy of communications, authentication of identity, and viable electronic commerce in a...

...are encouraged to see the industry working with the PICA-PKCS process to establish Internet **security** specifications to offer an open standard, and we look forward to participating in the process to lead its impact on Java," said Li Gong, **security** architect at JavaSoft, a business unit of Sun Microsystems, Inc.

"Our goal is to integrate strong **security** into all applications, ranging from commercial off-the-shelf to custom legacy applications," said Brad...

... Networks. "Towards that end, Nortel will be contributing APIs developed for the Entrust family of **encryption** and key management products, as well as our experience gained with real world solutions, to...

... WebFORCE Group Marketing Manager at Silicon Graphics, said "the recent proliferation of specifications in the **cryptography** arena has not been beneficial to our WebFORCE Internet Server customers or to the industry...

... Our Novell Directory Services (NDS) represents the world's largest commercial use of public key **cryptography** and is available on multiple platforms. PICAA will make it easier for developers to provide...

... provide to our customers," said Don Rothwell, vice president and director of Motorola's Information **Security** Operations. "PICA will allow exciting, new applications to reach the market more quickly than previously possible."

RSA Data **Security** , Inc., a wholly owned subsidiary of **Security** Dynamics Technologies, Inc., is the world's brand name for **cryptography** , with more than 75 million copies of RSA **encryption** and authentication technologies installed and in use worldwide.

RSA technologies are part of existing and...

... develops and markets platform-independent developer's kits and end-user products and provides comprehensive **cryptographic** consulting services. Founded in 1982 by the inventors of the RSA Public Key **Cryptosystem** , the company is headquartered in Redwood City, Calif.

Apple Computer, Inc., a recognized innovator in...
...Wide Web: http://www.apple.com

IBM's SecureWay brand is a comprehensive portfolio of **security** offerings. Whether addressing a specific requirement or creating a total end-to-end solution, IBM... networks. Additional information can be found on our SecureWay homepage at http://www.ibm.com **security** .

JavaSoft, headquartered in Cupertino, CA, is an operating company of Sun Microsystems Inc. The company...

... and systems for secure communications, Nortel has built a team of world-leading experts in **cryptography** , **security** architecture and international standards.

Nortel's Enterprise Networks group provides custom-designed enterprise networks for...

...COMPANY NAMES (DIALOG GENERATED): Development ; Cray ; Enterprise Networks ; EDI ; IBM ; IEEE ; ISO ; IT4 ; JavaSoft ; Lotus ; Microsoft ; Motorola 's Information **Security** ; Netscape Communications Corporation ;

Nortel Secure Networks ; Novell ; NDS ; Our Novell Directory Services ; PICA Alliance ; RSA Data **Security** Inc ; **Security** Dynamics Technologies Inc ; Silicon Graphics Inc ; Sun Microsystems Inc ; WebFORCE Group Marketing ; World Wide Web

24/3,K/10 (Item 2 from file: 636)

03392180
RSA DATA SECURITY: **Announcing a PICA** crypto-**alliance**
M2 Presswire Oct 18, 1996
WORD COUNT: 1620
PUBLISHER: M2 Communications

RSA DATA SECURITY: **Announcing a PICA** crypto-**alliance**

M2 PRESSWIRE-18 October 1996-RSA DATA **SECURITY** : Announcing a PICA **crypto** -alliance -- With Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics (C)1994...

... Silicon Graphics jointly announced their support for an effort code-named PICA, or "Platform-Independent **Cryptography** API." PICA builds on RSA's widely-adopted Public Key **Cryptography** Standards (PKCS) process and technology submissions from several companies.

The PICA alliance has been formed primarily to address potential interoperability problems that may arise as **cryptographic** technology moves into the mainstream software products of competing vendors. With open development meetings scheduled for later on this year, PICA vendors will attempt to "build bridges" between their differing **crypto** approaches, and will look for ways to simplify the way developers use **cryptography** on different platforms.

The PICA specification will be designed to allow developers to introduce open, cross-platform, application **independent** **security** in the same way that they introduce other features like graphics, **communications** , and networking **protocols** . PICA should enable developers to add **security** features such as SSL, DES, and smartcards to electronic commerce, banking, EDI and other applications...

... PICA will also be designed to make the task of developing differing domestic and exportable **security** requirements much easier.

Jim Bidzos, RSA President, said: "The original PKCS group, with members including...

... Graphics, Sun and many others, has been a place where competitors can work together on **crypto** specifications since its formation in 1991. "It is anticipated that the new PICA efforts will...

... The industry-wide effort is an important step towards simplifying the way developers work with **cryptography** ," he continued "Once a niche application, sophisticated **cryptography** is making its way into even the seemingly most pedestrian Internet applications -- and **crypto** is an important component in hot emerging segments such as electronic commerce, Internet EDI and electronic cash."

"This is an exciting time for **cryptography** . The PICA effort will better enable IBM's SecureWay **cryptographic** infrastructure to provide a less complex, more modular way for developers to build applications which make the Internet safe for business," said Kathy Kincaid, Director of I/T **Security** Programs for IBM.

"This will do for **security** what HTML did for the Web," said Mike Homer, VP Marketing for Netscape. "Netscape is happy to announce that our client

Networks ; Novell ; NDS ; Our Novell Directory Services ; PICA Alliance ; RSA RSA Data **Security** Inc ; **Security** Dynamics Technologies Inc ; Silicon Graphics Silicon Graphics Inc ; Sun Microsystems Inc ; WebFORCE Group Marketing ; With...

24/3,K/11 (Item 3 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

03391042
IBM JOINS APPLE, RSA, NETSCAPE IN PICA CRYPTO-**ALLIANCE**
Report on IBM Oct 23, 1996 V. 13 NO. 42
ISSN: 0742-5341 WORD COUNT: 235
PUBLISHER: DataTrends Publications, Inc

IBM JOINS APPLE, RSA, NETSCAPE IN PICA CRYPTO-**ALLIANCE**

INTEROPERABILTY AND **CRYPTOGRAPHY** : IBM, Apple, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics jointly announced support for an effort code-named PICA, or "Platform-Independent **Cryptography** API."

PICA builds on RSA's Public Key **Cryptography** Standards (PKCS) process and technology submissions from several companies.

The PICA alliance has been formed primarily to address potential interoperability problems that may arise as **cryptographic** technology moves into the mainstream software products of competing vendors. With open development meetings scheduled for later on this year, PICA vendors will attempt to "build bridges" between their differing **crypto** approaches, and will look for ways to simplify the way developers use **cryptography** on different platforms.

The PICA specification will be designed to allow developers to introduce open, cross-platform, application **independent security** in the same way that they introduce other features like graphics, **communications** , and networking **protocols** . PICA should enable developers to add **security** features such as SSL, DES, and smartcards to electronic commerce, banking, EDI and other applications...

... PICA will also be designed to make the task of developing differing domestic and exportable **security** requirements much easier.

"This is an exciting time for **cryptography** ," said Kathy Kincaid, Director of I/T **Security** Programs for IBM. "The PICA effort will better enable IBM's SecureWay **cryptographic** infrastructure to provide a less complex, more modular way for developers to build applications which...

24/3,K/12 (Item 1 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

06013524
Beyond Technology, What Online Companies Can Do To Reassure Customers: Net transaction security: **A state of mind**
CommunicationsWeek Feb 19, 1996 p. IA7
ISSN: 0746-8121
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 973

Beyond Technology, What Online Companies Can Do To Reassure Customers: Net transaction security: **A state of mind**

... Web sites, there are several things to consider. One is the selection of a transport **protocol** : Private **Communication** Technology, Secure Sockets Layer or Secure-HyperText Transfer Protocol (see sidebar).

Another is deciding whether to bypass a transport protocol for an **independent security** system, say, licensing RSA Data **Security** Inc.'s data **security** algorithms directly.

For smaller businesses--for example, mail-order companies dwarfed by the catalog operations...

...be used to process the order.

At the same time, advocates and marketers of data-**security** products assert it is important to look beyond a given software code and move into a **security** consciousness. Unless businesses are aware of the various possibilities for computer-related crimes, more than...

... Stewart, chief technology officer at back-office software provider Open Market Inc., in Cambridge, Mass. "**Encryption** is a tool that is trying to help you do those things, but it's...

...less-than-honest employees at a given merchant, Stewart said.

But there is a chance **security** could be breached before the transaction even is secured, he added, so companies should be...

... about this kind of thing leads us not just to developing the current round of **encryption** , Stewart said, but toward other options, including smart cards, which he predicted will come online...

...Web sites, there are several things to consider. One is the selection of a transport **protocol** : Private **Communication** Technology, Secure Sockets Layer or Secure-HyperText Transfer Protocol (see sidebar). Another is deciding whether to bypass a transport protocol for an **independent security** system, say, licensing RSA Data **Security** Inc.'s data **security** algorithms directly.

For smaller businesses--for example, mail-order companies dwarfed by the catalog operations...

...be used to process the order.

At the same time, advocates and marketers of data-**security** products assert it is important to look beyond a given software code and move into a **security** consciousness. Unless businesses are aware of the various possibilities for computer-related crimes, more than...

...Stewart, chief technology officer at back-office software provider Open Market Inc., in Cambridge, Mass. "**Encryption** is a tool that is trying to help you do those things, but it's...

...less-than-honest employees at a given merchant, Stewart said.

But there is a chance **security** could be breached before the transaction even is secured, he added, so companies should be...

...about this kind of thing leads us not just to developing the current round of **encryption** , Stewart said, but toward other options, including smart cards, which he predicted will come online...

...First you have a policy, then you have access control, then you have stuff like **encryption** , then you've also got to have a feedback loop, such as audit trails and...

...to software developer David Bodley at South Florida Mall in Miami, is to pinpoint where **security** breaches are likely to occur. He maintained that hacking individual messages is not very profitable...

...marketing at eShop Inc., an online shopping service based in San Mateo, Calif., settling the **security** question didn't lie in which **security** algorithm to use. Using both the Internet and X.25 dial-up services, eShop developed...

...independently to provide access and process transactions.

Rather than settling on one algorithm to ensure **security** , eShop instead licensed the Toolkit for Interoperable Privacy-Enhanced Messaging from RSA Data **Security** , in Redwood City, Calif. By encrypting messages, Weinstein said, eShop is able to offer a guarantee of **security** to its

customers. "No matter how you access us, you're guaranteed secure transactions. If...

...ll reimburse you. We tackled the perception issue straight on." (See story, page IA6.)
How **security** is perceived is more important than the specific technology, Weinstein added.
"Our personal focus is...

...Agreeing with Bodley and Stewart, Weinstein said the transaction isn't the only area of **security** in which businesses should concentrate.
"It's important that people use their heads when dealing...

24/3,K/13 (Item 2 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

02065230
THE FC-1000 SERIES FROM EFM OFFERS ULTIMATE IN USER FLEXIBILITY
News Release October 17, 1988 p. 1

...specifications. The EFM series of FC-1000 systems come complete with keypad selectable RS-232C **communications protocol** and two analog and pulse outputs per channel. Each unit has an LCD which displays volumetric flow data and temperature as well as cumulative totals for both **independent** channels. The **security** features of the FC-1000 are unique to the system. They include protection of all...

24/3,K/14 (Item 1 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

06056911 SUPPLIER NUMBER: 13567536
Implementation of the comprehensive integrated security **system for computer networks. (3rd Joint European Networking Conference)**
Muftic, Sead
Computer Networks and ISDN Systems, v25, n4-5, p469(7)
Nov, 1992
ISSN: 0169-7552 LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

Implementation of the comprehensive integrated security **system for computer networks. (3rd Joint European Networking Conference)**

ABSTRACT: The comprehensive integrated **security** system (CISS) was developed to provide computer system protection model for information management applications. CISS was based on the International Organization for Standardization/Open Systems Interconnection (ISO/OSI) **Security** Architecture model and complies with TCP/IP **communications protocol** recommendations. The model provides for an efficient and operating-environment-**independent security** applications and components.

...DESCRIPTORS: Safety and **security** measures...
...**Security** systems

26/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00938834 95-88226
Cryptanalysis and protocol failures
Simmons, Gustavus J
Communications of the ACM v37n11 PP: 56-65 Nov 1994
ISSN: 0001-0782 JRNL CODE: ACM
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 12688.01
WORD COUNT: 7170

...TEXT: system to the server along with a request for the server to set up a **secure channel** to B. The server contacts B, who generates a (random) session key and encrypts it...

... other subscriber, C, who has eavesdropped on the three ciphers involved in setting up the **secure channel** between A and B can easily recover the session key they are using. This requires...

... in advance that whenever D receives a request from the server to set up a **secure channel** with C, D will return a session key known to C. This means not that...

...mod n)mod n,
and send it to the server with a request that a **secure channel** be set up between C and D. In preparation for later use, C computes r...detection. All of this has taken place in the time required to set up a **secure channel** on the net, and has been unconditionally concealed from detection by the server. It might...

... the three ciphers that passed over the channel in the course of setting up the **secure** (?) **channel** between A and B. What C has done is to use the protocol to trick... of the "don't care" states as are useful can be included in the simplification **process** . In the **second** example based on the Simmons protocol, the covert channel for B might well have been...

26/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00759575 94-08967
A public key extension to the Common Cryptographic Architecture
Le, An V; Matyas, Stephen M; Johnson, Donald B; Wilkins, John D
IBM Systems Journal v32n3 PP: 461-485 1993
ISSN: 0018-8670 JRNL CODE: ISY
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 3072.00
WORD COUNT: 16326

...TEXT: eliminated the need to transport secret keys between communicating parties in order to establish a **secure channel** . When a pair of users A and B wishes to establish a **secure channel** , each user sends his or her public key to the other over the open channel...

... and economical using a simple, widely known protocol. When a device wishes to establish a **secure channel** , it first generates a public and private key pair. The public key is sent to...appearance of randomness in the encrypted value of K. The long control vector C is **first processed** by a hashing function h to produce a 128-bit vector H = h(C). The...

26/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00747520 93-96741
Internet Privacy Enhanced Mail
Kent, Stephen T
Communications of the ACM v36n8 PP: 48-60 Aug 1993
ISSN: 0001-0782 JRNL CODE: ACM
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 12688.01
WORD COUNT: 9143

...TEXT: encoding is employed for this field as is applied to the message content).

ENCRYPTION

The **second** PEM **processing** step also provides message encryption, if selected by the originator. This processing is performed only...implying that the user holds a public key obtained through some out-of-band, integrity **secure channel** (not through an untrusted network).

A certificate, like a credit card, does not remain valid...

26/3,K/4 (Item 1 from file: 624)
DIALOG(R)File 624:McGraw-Hill Publications

0699265
Securing E-Mail With Encryption: PGP and ViaCrypt PGP security methods are the standards to go by
Lan Times September 25, 1995; Pg 138; Vol. 12, No. 19
Journal Code: LAN ISSN: 1040-5917
Section Heading: Hands-On
Word Count: 1,391 *Full text available in Formats 5, 7 and 9*

BYLINE:
Al Berg

TEXT:
...known to third parties is difficult--the key usually has to be sent over a **secure channel** and a lot of extra security precautions are needed.

The RSA algorithm used by PGP...

...only to the key owner.

Users create their two keys when running PGP for the **first** time. This **process** takes less than 10 minutes.

Once users have created a key set, they need to...

26/3,K/5 (Item 2 from file: 624)
DIALOG(R)File 624:McGraw-Hill Publications

0249074
AN OVERVIEW OF CRYPTOGRAPHY: Technology provides network privacy
Lan Times February, 1990; Pg 100; Vol. VII, Issue II
Journal Code: LAN ISSN: 1040-5917
Section Heading: Network Technology
Word Count: 2,611 *Full text available in Formats 5, 7 and 9*

BYLINE:
D. JAMES BIDZOS AND BURT S. KALISKI JR.

TEXT:
... How does the originating party transmit the secret key to the other party, since no **secure channel** exists at his or her point? This problem compounds when the communicating parties number in... less than 250 milliseconds.

Note that in the authentications protocol described above, the 1.5-**second** signature **process** is required only upon login by the user, and, although done only once, can be...

28/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01152743 98-02138

A new way to upgrade SCADA
Komisarek, Jim; Blecke, Charles
Transmission & Distribution v47n13 PP: 30-36 Dec 1995
ISSN: 0041-1280 JRNL CODE: TMD
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 12343.02
WORD COUNT: 1730

...TEXT: that takes advantage of the unique dual-processing architecture inherent in the M4RTU. While a **second processor** performs I/O interfacing and control of signals from the substation, the M4RTU's high...

... Redac 70H. The flexibility of the Opto 22 system also frees WPS to change EMS **communications protocol** in the future.

Man-Machine Interface

WPS developed the operator interface with the Mistic MMI...

28/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00908564 95-57956
Digital signatures: Signing and notarizing electronic forms
Theofanos, Mary F; Phillips, John T
Records Management Quarterly v28n2 PP: 18-22+ Apr 1994
ISSN: 1050-2343 JRNL CODE: RMQ
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 6778.00
WORD COUNT: 3587

...TEXT: ID), date/time stamp, and document ID, followed by encryption of this information. A secure **communications protocol** based on the Kerberos method for authentication, authorization, and accounting on a network was used to protect the information during the signature generation **process** . The **second** level of authentication provides a notary ability, similar to a notary in the paper world...

28/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00858786 95-08178
Service designs for quality: Integrated-process necessity
Georgantzas, Nicholas C; Madu, Christian N
Mid-Atlantic Journal of Business v30n1 PP: 55-80 Mar 1994
ISSN: 0732-9334 JRNL CODE: JBZ
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM 5137.01
WORD COUNT: 7981

...TEXT: redesign their services by challenged fundamental tradeoff assumptions about dependability, efficiency, flexibility, and service quality.

Second , the integrated **process** of modeling provides a forum for communicating and debating assumptions, and a **communication protocol** for doing so. So, it enables learning, and improves judgment and intuition (Senge, 1990). The...

28/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

00540245 91-14589
DSP May Spell Relief for Urban Cellular Congestion

Cox, Steve; Fine, Bob
Telephony v220n9 PP: 18-26 Mar 4, 1991
ISSN: 0040-2656 JRNL CODE: TPH
AVAILABILITY: Photocopy available from ABI/INFORM 1108.00
WORD COUNT: 2298

...ABSTRACT: the problems in overpopulated mobile telephone systems. In a digital system, the speech signal is **first processed** digitally by compression algorithms and error correction techniques. The resulting information is used to modulate...

... the late 1980s, a standards group, Groupe Special Mobile, was formed to select a standard **communications protocol** for the proposed pan-European system. ...

28/3,K/5 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

00632289 CMP ACCESSION NUMBER: EET19891218S0400
LANs throttle up to meet broader applications
RAY WEISS
ELECTRONIC ENGINEERING TIMES, 1989, n 569, 37
PUBLICATION DATE: 891218
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: DES
WORD COUNT: 2576

... by Larry Green, a key figure at Silicon Graphics. Protocol Engines aims to speed up **communications protocol** processing by taking a two-pronged approach to minimizing protocol **processing** overhead.
First , its designers are defining a compressed protocol. The express transport protocol (XTP) simplifies the earlier...

28/3,K/6 (Item 1 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00545674 00545674

SCSI CONNECTIVITY LIMITATIONS SOLVED WITH NEW, HIGH SPEED ARCHITECTURE FROM VICOM SYSTEMS

PR Newswire
DATELINE: LAS VEGAS Nov 13, 1995 WORD COUNT: 668

...using industry standard SCSI or SSA
interfaces. With multiple simultaneous transmission rates of
640Mbits per **second** , increased **node** - to-node distances and unlimited
devices per channel, SLIC finally enables the promised benefits of...

...and SSA products. "We expect a number of SLIC
implementations will be as an independent **communications protocol** to
take advantage of the 640Mbit per second transfer rate and its
support of simultaneous...

...high performance communications environments
independent of LANs, WANs or other networks and is the only
communications protocol that supports simultaneous transmissions.
SLIC incorporates advanced SCSI features such as command processing,
tagged queuing...

28/3,K/7 (Item 2 from file: 621)

DIALOG(R)File 621:IAC New Prod.Annou.(R)

00329826 00329826

VMEbus Dual Processor Single Board Computer Delivers 10 MIPS for Real-time and Telecommunication Functions

News Release
DATELINE: Pittsburgh, PA May 11, 1992 WORD COUNT: 937

...ideal for real-time
embedded applications, based on the functionality of its 68EC030 microprocessor. The **second processor** -- a 68302 intelligent multiprotocol processor (IMP) -- offers efficient data communications, including network communications control. "A...

...a smart universal protocol controller, handling I/O for virtually all synchronous and asynchronous data **communications protocols** in ISDN, X.25 and Fieldbus environments. Meanwhile, the 68EC030 handles I/O and processing...

28/3,K/8 (Item 3 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00275122 00275122

BANYAN AND COMPAQ TEAM UP TO DELIVER POWERFUL PC NETWORK SOLUTION

News Release
DATELINE: DALLAS, TX September 11, 1990 WORD COUNT: 1653

...mail gateways
-SNA, bisynch, and asynch terminal emulation
-TCP/IP, X.25, Appletalk, and other **communications protocols**
This consolidation yields two key benefits: A reduced investment in LAN hardware and complexity; and...

...server to support their user communities. As the network grows, customers can simply add the **second processor** (in the case of the SYSTEMPRO) in order to increase the capacity and performance of...

28/3,K/9 (Item 4 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00212241 00212241

AT&T INTRODUCES DEFINITY 75/85 COMMUNICATIONS SYSTEM

PR Newswire
DATELINE: WASHINGTON, DC February 6, 1989 WORD COUNT: 1014

...on common port hardward for line connections, DEFINITY 75/85 Communications System offers customers two **processor** options. The **first** option, called DEFINITY Generic 1, is for intermediate-sized businesses. The second option, called DEFINITY...

...the DEFINITY
family. The company added two new sets to its 7400 series of Digital **Communications Protocol** (DCP) terminals. DCP has successfully brought AT&T customers advanced ISDN-like functions since 1984...

28/3,K/10 (Item 5 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00154153 00154153

PLEXUS COMPUTERS INTRODUCES XDP SYSTEM INTEGRATING NUMEROUS TYPES OF BUSINESS INFORMATION

DATELINE: San Jose, CA March 30, 1987 WORD COUNT: 1212

...March 30, 1987 -- Plexus (R) Computers, Inc., today
introduced the Plexus XDP (TM) Extended Data **Processing** System, the **first** comprehensive commercial computer system that integrates and manages diverse types of data and peripherals.
The...devices; shared laser printers; an optical
character recognition device; and support for industry-standard
network **communications protocols** . All are available from Plexus.
Sales and Service
Prices for Plexus XDP Systems range from...

28/3,K/11 (Item 6 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00138710 00138710

CCI ANNOUNCES PRICE/PERFORMANCE-LEADING SUPERMINICOMPUTERS NEW COMPACT MODELS TARGETED TO RESELLERS

DATELINE: IRVINE, CA November 7, 1986 WORD COUNT: 673

...success next year and beyond."
The POWER 6/32S at 5 MIPS (million of instructions **processed** per **second**) is field upgradeable to the 8-MIPS POWER 6/32SX. A single system offers connectivity...

...Th.e new systems are also the first to incorporate CCI's new MPCC (Multi-**Protocol Communications** Controller). This controller permits concurrent use of asynchronous, bisynchronous, and bit-oriented protocols, and provides...

28/3,K/12 (Item 7 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00110140 00110140

BUNKER RAMO UNVEILS BRAND-NEW BROKERAGE NETWORK, SUPERNET

DATELINE: New York, NY September 11, 1985 WORD COUNT: 1437

...first automated quotation
display; the first voice response system for the American Stock Exchange; the **first** desktop distributed **processing** system for on-line quotes; the first electronic stock market for NASD; and the first...

...to open its network
architecture to office automation systems from vendors that support industry-standard **communication protocols** . Resulting from IBM's dominant force in the office automation market, Bunker Ramo will provide...

28/3,K/13 (Item 1 from file: 275)

DIALOG(R)File 275:IAC(SM) Computer Database(TM)
(c) 1998 Info Access Co. All rts. reserv.

01455770 SUPPLIER NUMBER: 11471517 (USE FORMAT 7 OR 9 FOR FULL TEXT)
RISC champions challenge Moto in embedded control. (RISC vendors challenge Motorola's 68000 CISC processor in embedded control systems) (includes related articles on Clearpoint Research's Little Dipper multiport media access control learning bridge router and on when to use a RISC-based processor in an embedded system) (Cover Story)
Child, Jeff; Wilson, Dave
Computer Design, v30, n13, p98(9)
Oct, 1991
DOCUMENT TYPE: Cover Story ISSN: 0010-4566 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5417 LINE COUNT: 00416

... system. Three of them are used together with a custom coprocessor simply to perform video **processing** . The **first** i960CA is used to calculate different information between video frames. The second controls the discrete...

...additional i960CA processor acts as the communications multiplexer and implements the CCITT standard H.221 **communications protocol** . The i960CAs are front-ended by an Intel 386 so that the user can teleconference ...

28/3,K/14 (Item 2 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)
(c) 1998 Info Access Co. All rts. reserv.

01426391 SUPPLIER NUMBER: 10535549 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Printer sharing made simple. (Hands-on) (tutorial)
Rosch, Winn L.
PC Sources, v2, n4, p489(3)
April, 1991
DOCUMENT TYPE: tutorial ISSN: 1052-6579 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2330 LINE COUNT: 00179

... time to print a file.
Readying your serial port for printing is a two-step **process** . **First** , set its speed and other **communications protocol** parameters, then redirect print commands to the port. Remember, you must set the communications parameters...

28/3,K/15 (Item 3 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)
(c) 1998 Info Access Co. All rts. reserv.

01389078 SUPPLIER NUMBER: 09407920 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Control network keeps nodes simple.
Bursky, Dave
Electronic Design, v38, n23, p139(3)
Dec 13, 1990
ISSN: 0013-4872 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1812 LINE COUNT: 00144

... To bring the LONs to reality, Echelon defined several chips and a robust yet flexible **communication protocol** . It also created an easy-to-use set of network setup and development tools. At...

...two Echelon-defined Neuron single-chip devices. Each chip offers communications, control, and I/O **processing** . The **first** two Neuron **processors** are jointly defined by Echelon with Motorola and Toshiba-the companies that will actually manufacture...

28/3,K/16 (Item 4 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)

01290831 SUPPLIER NUMBER: 07070594 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Top 10 bank software growth companies. (company profile)
Landis, Ken
Computers in Banking, v6, n2, p26(12)
Feb, 1989
DOCUMENT TYPE: company profile ISSN: 0742-6496 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 10767 LINE COUNT: 00873

... price/performance ratio--is helping them compete.
The decentralization of information management as well as **processing** is the **second** trend. Decentralization requires complex data **communication protocols** , as well as inter-application standards such as IBM's Systems Application Architecture. "Users and...

28/3,K/17 (Item 1 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

04684956
Intel Launching Long-Range Supercomputer Project
Intel: Supercomputing program aims to reach teraFLOPS performance by 1997-98
Electronic News October 25, 1993 p. 8
ISSN: 1061-6624
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 241

... a superscalar structure, or groups of five or six less expensive MPUs in symmetrical multiprocessing **nodes** .
The **first** prototype, planned for late 1995, has performance targets of 600 gigaFLOPS peak speed with 350...

... selected applications. Each MPU node will contribute about 150 megaFLOPs, and the system will use **communication protocols** to reduce message passing latency and access remote memory.
A second prototype planned for 1996...
?

```
File 275:IAC(SM) Computer Database(TM) 1983-1998/Dec 01
         (c) 1998 Info Access Co
File 674:Computer News Fulltext 1989-1998/Nov W5
         (c) 1998 IDG Communications
File 647:CMP  Computer Fulltext 1988-1998/Nov W2
         (c) 1998 CMP
File  15:ABI/INFORM(R) 1971-1998/Dec 01
         (c) 1998 UMI
File  16:IAC PROMT(R) 1972-1998/Dec 01
         (c) 1998 Information Access Co.
File   9:Business & Industry(R) Jul 1994-1998/Dec 01
         (c) 1998 Resp. DB Svcs.
File 621:IAC New Prod.Annou.(R) 1985-1998/Dec 01
         (c) 1998 Information Access Co
File 636:IAC Newsletter DB(TM) 1987-1998/Dec 01
         (c) 1998 Information Access Co.
File 148:IAC Trade & Industry Database 1976-1998/Dec 01
         (c) 1998 Info Access Co
File 624:McGraw-Hill Publications 1985-1998/Nov 25
         (c) 1998 McGraw-Hill Co. Inc

Set     Items   Description
S1         24   (INDEPENDENT(N2)LAYER?) (S) (JAVA OR ENCRYPTION?)
S2         18   RD (unique items)
?
```

2/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275:IAC(SM) Computer Database(TM)

02140765 SUPPLIER NUMBER: 20206035 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Understanding the DCOM wire protocol by analyzing network data packets. (the Distributed COM Object RPC network protocol) (Technology Information)(Technical)
Eddon, Guy; Eddon, Henry
Microsoft Systems Journal, v13, n3, p45(13)
March, 1998
DOCUMENT TYPE: Technical ISSN: 0889-9932 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 8796 LINE COUNT: 00754

... see Figure 3).
As you can see in Figure 3, DCOM is not really an **independent** network protocol **layered** on top of the RPC protocol. Instead, DCOM merges with the RPC header and data...

...of the OSF DCE RPC network protocol. For example, the authentication, authorization, and message integrity/**encryption** features of RPC are present in ORPC.
The ORPC protocol extends the standard RPC protocol...

2/3,K/2 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01109420 CMP ACCESSION NUMBER: EET19961104S0066
HTTP, Java provide run-time control
Steven Houtchens, Director of New Technology, Integrated Systems Inc., Santa Clara, Calif.
ELECTRONIC ENGINEERING TIMES, 1996, n 926, PG60
PUBLICATION DATE: 961104
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Embedded Systems
WORD COUNT: 1432

... native code methods.
Our example of the embedded network switch uses the flexibility of the **Java** language to define distinct and separate **layers** of hardware-**independent** application code, and native, hardware-dependent code. This also has the side benefit of maintaining...

...execution in the native classes, and allowing the slower supervisory functions to be coded in **Java** .
In addition to the network-switch example, Java can be used for warehouse-inventory control...

2/3,K/3 (Item 1 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01646725 02-97714
Ten Commandments for converting your intranet into a secure extranet
Lister, Tom
UNIX Review's Performance Computing v16n8 PP: 37-39 Jul 1998
JRNL CODE: URPC
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM
WORD COUNT: 1799

...TEXT: using the Internet, requiring that data be encrypted as it travels across the untrusted network.

Encryption can be performed at the network level using VPN products such as encrypting routers or...

... browsers and servers supporting Secure Sockets Layer (SSL). The advantage of VPN products is their **layer** of application-- **independent encryption** for all network traffic between the connected LANs. Unfortunately, they require specialized hardware or software...

2/3,K/4 (Item 2 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01512975 01-63963
IBM's San Francisco project
Kara, Dan
Software Magazine v17n11 PP: 104, 103 Oct 1997
ISSN: 0897-8085 JRNL CODE: SMG
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM
WORD COUNT: 1512

ABSTRACT: IBM's recently released "San Francisco Project" is best described as **Java** -based, reusable, object-oriented business components for commercial applications, along with an execution framework. San...

... a reusable substrate or functional lattice for other San Francisco components. The Common Business Objects **layer** consists of **independent** , generalized business objects and frameworks common to a variety of application types that can be...

... substructure, designed by a large number of vendors, on which ISVs and other can build **Java** -based, commercial, networked applications.

2/3,K/5 (Item 3 from file: 15)
DIALOG(R)File 15:ABI/INFORM(R)

01333173 99-82569
HTTP, Java provide run-time control
Houtchens, Steven
Electronic Engineering Times n926 PP: 60, 77 Nov 4, 1996
ISSN: 0192-1541 JRNL CODE: ELET
AVAILABILITY: Fulltext online. Photocopy available from ABI/INFORM
WORD COUNT: 1443

...TEXT: native code methods.

Our example of the embedded network switch uses the flexibility of the **Java** language to define distinct and separate **layers** of hardware-**independent** alr plication code, and native, hardware-dependent code. This also has the side benefit of native classes, and allowing the slower supervisory functions to be coded in **Java** .

In addition to the network-switch example, Java can be used for warehouseinventory control applications...

2/3,K/6 (Item 1 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

07571501 SUPPLIER NUMBER: 50105926
Java Startup Financed by Esther Dyson Launches First JFC-based Java Development Tool -- NetBeans, Inc. --.
Business Wire June 22, 1998 p. 6221006

FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 759

... including NT, UNIX, Linux, OS/2, Win95, and Solaris. The system is built from several **independent layers** , and is designed to be open and easily extendible. The IDE is presented in the...

... within the system - editing, compilation, execution and debugging. The entire IDE GUI is based on **Java** Foundation Classes and takes advantage of all its impressive features, including a pluggable look and feel and a rich component set. "Using **Java** technology for NetBeans IDE allowed us to build a product that leverages the 'Write Once, Run Anywhere(TM)' capability of the **Java** platform," said Roman Stanek, founder and CEO of NetBeans.
...
...including NT, UNIX, Linux, OS/2, Win95, and Solaris. The system is built from several **independent layers** , and is designed to be open and easily extendible. The IDE is presented in the...

...within the system - editing, compilation, execution and debugging. The entire IDE GUI is based on **Java** Foundation Classes and takes advantage of all its impressive features, including a pluggable look and feel and a rich component set. "Using **Java** technology for NetBeans IDE allowed us to build a product that leverages the 'Write Once, Run Anywhere(TM)' capability of the **Java** platform," said Roman Stanek, founder and CEO of NetBeans.
NetBeans' distributed computing features also mean...

2/3,K/7 (Item 2 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

06702804 SUPPLIER NUMBER: 06709227
CompuServe Network Services L2F
Chen, Elaine; Bournellis, Cynthia
Electronic News (1991) Feb 24, 1997 p. 044
ISSN: 1061-6624
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 102

... up customers based on Cisco Systems' Layer 2 Forwarding (L2F) technology. L2F is a media **independent Layer** 2 tunneling protocol offered in Cisco's IOS software. Layer 2 tunneling protocols provide dial
...

...and filtering are all controlled by the customer's own network. Existing technologies, such as **encryption** , will run transparently end-to-end over Layer 2 tunnels ensuring privacy and confidentiality.
...

2/3,K/8 (Item 3 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

06505322
HTTP, Java provide run-time control
Java, HTTP have applications in connecting embedded devices to Internet
Electronic Engineering Times Nov 4, 1996 p. 60
ISSN: 0192-1541
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 1418

...native code methods.
Our example of the embedded network switch uses the flexibility of the **Java** language to define distinct and separate **layers** of hardware-**independent** application code, and native, hardware-dependent code. This also has the side benefit of maintaining classes, and allowing the slower supervisory functions to be coded in **Java** .

In addition to the network-switch example, Java can be used for warehouse-inventory control...

2/3,K/9 (Item 4 from file: 16)
DIALOG(R)File 16:IAC PROMT(R)

05956349
V-ONE Corp. Defines a New Class of Security Products: Security Middleware; Industry's First Security Middleware product, SmartGATE, will be demonstrated at RSA Conference in San Francisco.
Business Wire Jan 16, 1996 p. 01160206
FULL TEXT AVAILABLE IN FORMAT 7 OR 9 WORD COUNT: 877

...frees the application developer from battling compatibility and security problems. "By relying on a vendor-**independent layer** that negotiates secure application sessions, an application can instantly take advantage of new technologies in **encryption** and authentication as they emerge," Ranum said.
Ranum noted that "V-ONE is trying to...

2/3,K/10 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R) Jul

02052307 (USE FORMAT 7 OR 9 FOR FULLTEXT)
SunConnect: Moving Financial Services to the Web
(In 1996, over 7 mil US households were prime candidates for PC-based home banking and bill payment services; it is projected that the number will exceed 20 mil by 2000)
US Banker, v 108, n 1, p S2+
January 1998
DOCUMENT TYPE: Journal ISSN: 0148-8848 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2378

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...conduct commerce on a public network and the SWC module gets there by applying several **independent layers** of **encryption** and authentication to all communications involved in a transaction. The SWC module permeates the entire...

...between different servers or between servers and traditional legacy data processing systems. In particular, the **Java** Electronic Commerce Framework adds to essential **Java** security capabilities for the emerging world of electronic commerce.

The ITA module is at the...

2/3,K/11 (Item 1 from file: 621)
DIALOG(R)File 621:IAC New Prod.Annou.(R)

00878271 00878714

ObjectShare Expands Relationship with Applied Reasoning to Distribute New Products; Two Additional Products to Compliment ObjectShare's VisualWorks.

Business Wire
DATELINE: IRVINE, Calif. April 2, 1998 WORD COUNT: 719

...fully distributed client-server application development
and server-side processing. GeoSynchrony offers a flexible,
database-**independent** persistence **layer** and full map zooming and
optimized spatial and non-spatial queries. GeoSynchrony was released
in...

...object-oriented
solutions for network computing. With complete support for industry
standards using Smalltalk or **Java** , the company offers its
development environments, frameworks, along with consulting,
education and support services worldwide...

2/3,K/12 (Item 1 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

03055067
MOTOROLA BRINGS WIRELESS OPTIONS TO NOTES
Wireless Messaging Report Jan 30, 1996 V. 4 NO. 2
WORD COUNT: 941
PUBLISHER: BRP Publications

... Mobile Data Inc.) and cellular digital packet data (CDPD) networks.
Because it appears as an **independent** middle **layer** between Notes and the
wireless network, and because it does so through the use of...

...software does not change any of the features of Notes, including its use
of data **encryption** to prevent the interception of messages while in
transit.

Eventually, Motorola plans to extend the...

2/3,K/13 (Item 2 from file: 636)
DIALOG(R)File 636:IAC Newsletter DB(TM)

02716772
NETSCAPE TAKES WRAPS OFF NETSCAPE NAVIGATOR 1.1
The PCNetter March 1995 V. 10 NO. 3
ISSN: 0893-8075 WORD COUNT: 575
PUBLISHER: Architecture Technology Corporation

...dynamic data

- Additional security options, including an enhanced U.S.-only version with
non-exportable **encryption** technology, and secure Usenet news/conferencing
capabilities based on the application- **independent** Secure Sockets **Layer**
(SSL) Protocol; this protocol is compatible with Netscape's recently
published SSL source code reference...

2/3,K/14 (Item 1 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

09659964 SUPPLIER NUMBER: 19445944 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Isolation systems isolating companies' sensitive data. (Isolation Systems Inc.)
Venetis, Tom
Computer Dealer News, v13, n7, p48(1)
March 24, 1997
ISSN: 1184-2369 LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 414 LINE COUNT: 00035

... their infrastructure and lower costs."

The InfoCrypt Series consists of four modular software and hardware **encryption** products which work together to provide a secure data pipeline across a public network like the Internet. The products operate at the network **layer** and are **independent** of the network topology and the software and operating systems.

The InfoCrypt Enterprise base product...

2/3,K/15 (Item 2 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

09648140 SUPPLIER NUMBER: 18422715 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Emerging standards back virtual secure tunnels.
Barbetta, Frank
Business Communications Review, v26, n5, p30(2)
May, 1996
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1350 LINE COUNT: 00113

... similar to that of the earlier IEEE 802.10 standard--encapsulation formats, authentication headers, SDE **layer** specs, algorithm-**independent encryption** , security associations, virtual secure connections, etc. However, to date, the LAN bridge--oriented 802.10...

2/3,K/16 (Item 3 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

08119009 SUPPLIER NUMBER: 17376789 (USE FORMAT 7 OR 9 FOR FULL TEXT)
NETSCAPE ANNOUNCES INTERNATIONAL VERSIONS OF NETSCAPE NAVIGATOR 1.1
PR Newswire, p911NY030
Sep 11, 1995
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 689 LINE COUNT: 00080

... updated information -- such as stock quotes, weather maps and other dynamic data.

-- Security options including **encryption** technology and secure Usenet news/conferencing capabilities based on the application-**independent** Secure Sockets **Layer** (SSL) open protocol.

-- Enhanced Usenet news interface, including hierarchical newsgroup browsing and searching, optimizations for...

2/3,K/17 (Item 4 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

07852250 SUPPLIER NUMBER: 16926084 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Netscape unveils Netscape Navigator 1.1. (software)
Information Today, v12, n4, p61(1)
April, 1995
ISSN: 8755-6286 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 647 LINE COUNT: 00066

... dynamic data
Additional security options, including an enhanced U.S.-only version with non-exportable **encryption** technology, and secure Usenet news/conferencing capabilities based on the application-**independent** Secure Sockets **Layer** (SSL) protocol have also been added. This protocol is compatible with Netscape's recently published...

2/3,K/18 (Item 5 from file: 148)
DIALOG(R)File 148:IAC Trade & Industry Database

05441021 SUPPLIER NUMBER: 11238218 (USE FORMAT 7 OR 9 FOR FULL TEXT)
"Over there" for fun and profit. (Trade Shows)
Szathmary, Richard
Sales & Marketing Management, v143, n11, p161(2)
Sept, 1991
CODEN: SMMAD ISSN: 0163-7517 LANGUAGE: ENGLISH RECORD TYPE:
FULLTEXT; ABSTRACT
WORD COUNT: 20090 LINE COUNT: 01753

... is transported across the WAN. The 8023 Trestle operates at the Media Access Control (MAC) **layer** which is **independent** of higher-level protocols. An **encryption** option is available for "sensitive but unclassified" applications.

FOX-2

This is a 6.3...

?

```
File 256:SoftBase:Reviews,Companies&Prods. 85-1998/Oct
         (c)1998 Info.Sources Inc
File 278:Microcomputer Software Guide 1998/Nov
         (c) 1998 Reed Elsevier Inc.

Set     Items   Description
S1        147   (INDEPENDENT? OR SEPARATE?)(N2) (LAYER? OR PROTOCOL?)
S2       8078   SECURITY? OR ENCRYPTION? OR DECRYPTION? OR CRYPTO?
S3         24   (SECURE()CHANNEL? OR JAVA(N2)STREAM? OR JAVA()SECURE()CHAN-
              NEL?)
S4          7   (FIRST AND SECOND)(N2)(NODE? OR PROCESS?)
S5       1348   COMMUNICATION?(N)PROTOCOL?
S6          0   ((COMMUNICATION?)(N2)(CHANNEL? OR PROTOCOL?))(N50)(S2(N3)I-
              NDEPENDENT?)
S7          0   S3 AND S1
S8         10   S1 AND S2
S9          0   S8 AND S5
S10         0   S5 AND ((INDEPENDENT?) (N2) (ENCRYPTION? OR CRYPTO?))
S11         3   INDEPENDENT?(N5) (ENCRYPTION? OR CRYPTO?)
?
```

8/3,K/1 (Item 1 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)1998 Info.Sources Inc. All rts. reserv.

01640581 DOCUMENT TYPE: Product

PRODUCT NAME: VACMan/Server (640581)

VASCO Data **Security** Inc (621072
1919 S Highland Ave #118C
Lombard, IL 60148 United States
TELEPHONE: (630) 932-8844

RECORD TYPE: Directory

CONTACT: Erling Smedvig, VP North American Sales

REVISION DATE: 970603

VASCO Data **Security** Inc...

VACMan/Server is the first **protocol -independent** authentication, authorization and accounting solution for Windows NT, Windows 95, Netware and UNIX. Designed specifically...

DESCRIPTORS: Computer **Security** ; Remote Network Access; Network Administration Tools; Network Software; Local Area Networks; System Monitoring; Network Servers

8/3,K/2 (Item 2 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)1998 Info.Sources Inc. All rts. reserv.

00104045 DOCUMENT TYPE: Review

PRODUCT NAMES: Hydra Windows NT (656895); WinFrame Windows NT (672424); Liftoff Windows NT (673552)

TITLE: Options for multiuser NT on the rise
AUTHOR: Paone, Joe
SOURCE: LAN Times, v14 n21 p16(1) Oct 13, 1997
ISSN: 1040-5917
HOMEPAGE: http://www.lantimes.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 980228

...only works with NT 3.51, and thus cannot support Windows 95 users. Citrix's **protocol , Independent** Computing Architecture (ICI), supports non-Windows clients, but Hydra's new protocol T.SHARE/T...
...not found in Hydra, such as load-balancing, application configuration tools, user management features, and **security** . New Moon's Liftoff is expected to be released in 1998 and will be marketed...

8/3,K/3 (Item 3 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)1998 Info.Sources Inc. All rts. reserv.

00099596 DOCUMENT TYPE: Review

PRODUCT NAMES: WorkFlo Business System (210293); DocPageServer (660183); RightSite (660191); OPEN/image (416312); OPEN/stor (650196)

TITLE: Easing the Growing Pains of an Enterprise System
AUTHOR: Blecher, Joni
SOURCE: Imaging Magazine, v5 n12 p52(11) Dec 1996
ISSN: 1083-2912
HOMEPAGE: http://www.imagingmagazine.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 980130

...the system's ability to support a corporate infrastructure. A company's infrastructure should provide **security** for WAN users, and suitable systems for active and nonactive data storage are required. RightSite... ...jukeboxes for permanent archival storage, and OPEN/stor provides a centralized data storage that enhances **security** . OPEN/stor resides under the server, and is transparent to network users. It manages data...

...NT systems on the network. Among topics discussed are indexing or cataloging, replication, maintaining a **separate** annotation **layer** , and FileNet's products for document indexing.

8/3,K/4 (Item 4 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00094527 DOCUMENT TYPE: Review

PRODUCT NAMES: Microsoft SNA Server (472701)

TITLE: Point... Counterpoint: Gateway Products: The Only Way to Connect to..
AUTHOR: Walkley, Wayne
SOURCE: AS/400 Systems Management, v24 n6 p36(4) Jun 1996
ISSN: 1070-6097

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 980530

...is the extra maintenance and expense required, as well as the necessity of keeping two **separate layers** of **security** . SNA Server also limits choices because it can handle only Windows clients. The additional gateway ...

...DESCRIPTORS: NT; Communications Interfaces; Internetworking Software; Local Area Networks; IBM PC & Compatibles; IBM AS/400; Computer **Security** ; SNA; Network Software

8/3,K/5 (Item 5 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00083195 DOCUMENT TYPE: Review

PRODUCT NAMES: Internet (833029); Computer Security **(830071**

TITLE: Heavyweights duel on specs
AUTHOR: Moeller, Michael
SOURCE: PC Week, v12 n42 p63(2) Oct 23, 1995
ISSN: 0740-1604

HOMEPAGE: http://www.pcweek.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 960228

...**PRODUCT NAMES: 833029); Computer** Security (

...there are currently several competing protocols and specifications. MasterCard and Visa are competing with different **security** specifications, both of which are mutually incompatible. MasterCard, with IBM, Netscape, GTE, and CyberCash, has...

...usage of the Internet as a commercial platform, because merchants would have to support multiple **protocols . Separately** , Microsoft and Netscape are competing with different general **security** specifications. Microsoft's Private Communications Technology (PCT) will compete against Netscape's Secure Sockets Layer (SSL). PCT differs from SSL by separating authentication from **encryption** , thereby supporting stronger authentication schemes.

DESCRIPTORS: Internet; Computer **Security** ; Communications Standards; Internet Marketing; Public Networks; Electronic Funds Transfer; Computer Conferencing

8/3,K/6 (Item 6 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00075442 DOCUMENT TYPE: Review

PRODUCT NAMES: Instant Internet (551201)

TITLE: Easy Net Access for IP-Wary Managers
AUTHOR: Shimmin, Bradley F.
SOURCE: LAN Times, v12 n6 p25(2) Mar 27, 1995
ISSN: 1040-5917
HOMEPAGE: http://www.lantimes.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 970211

...administrators to provide workstation Internet links simply by plugging the device into a network. No **separate** Transmission Control **Protocol** /Internet Protocol (TCP/IP) stack is required. The administrator merely enters service provider data and...
...Internet Protocol address, and the product prohibits incoming TCP/IP from the Internet for enhanced **security** . A beta user testing the product with a router connection likes the higher communications speed...

8/3,K/7 (Item 7 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00069110 DOCUMENT TYPE: Review

PRODUCT NAMES: DEC OSF/1 (227005)

TITLE: What's Happenin', Dudes?
AUTHOR: Bourne, Philip E.

SOURCE: DEC Professional, v13 n9 p56(3) Sep 1994
ISSN: 0744-9216

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 960330

...2,500 applications have been ported to the environment. DEC also announced the Multi-Level **Security** Plus feature that extends C2 **security** and addresses some of the vulnerabilities of windowing and NFS. In April, Digital announced AdvantageClusters...

...software to DEC OSF/1. OpenStep is NeXT's proposed standard for an operating system **independent** application **layer** that runs on several host operating systems. Digital also plans to integrate OpenStep with ObjectBroker...

8/3,K/8 (Item 8 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00062823 DOCUMENT TYPE: Review

PRODUCT NAMES: Computer Security **(830071**

TITLE: Case Study: Multinet Gateway System
AUTHOR: Gerhart, Susan Craigen, Dan Ralston, Ted
SOURCE: IEEE Software, v11 n1 p37(3) Jan 1994
ISSN: 0740-7459
HOMEPAGE: http://www.computer.org/pubs/softare/sof

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 970930

PRODUCT NAMES: Computer Security **(**

...also provides mechanisms to protect sensitive information, and complies with the Department of Defense's **security** criteria. MGS was developed to achieve A-class certification, and contains many novel aspects. It was also the first attempt to distribute **protocols** over **separate** processors. The main **security** assertions are that the system accepts data only from input wires, and only if the data is consonant with **security** levels of the input wires. Furthermore, the system delivers data to an output wire only if it is derived from data received at input wires, and only if **security** levels are the same as the output wire. Also, the system will deliver data only to output wires, only if data is consonant with **security** levels of the output wires.

DESCRIPTORS: Computer **Security** ; Public Networks; Telecommunications; System Monitoring; Data Communications; Internet Utilities

8/3,K/9 (Item 9 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00058227 DOCUMENT TYPE: Review

PRODUCT NAMES: Carbon Copy for Windows 2.0 (359211); Close-Up/LAN 5.0 (203165); Netblazer (465976); CentrumRemote Remote Access Server (402907) ; Remote LAN Node (RLN) Access Server 2.0 (603252)

TITLE: Remotely Speaking
AUTHOR: Miller, Mark A.
SOURCE: Network World, v10 n43 p43(7) Oct 25, 1993
ISSN: 0887-7661
HOMEPAGE: http://www.nwfusion.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

REVISION DATE: 980530

...video compression. The Netblazer series of remote access servers offers strong options for management and **security** . Remote LAN Node 2.0 has an impressive **protocol -independent** , modular approach to remote LAN access. CentrumRemote's feature set is very comprehensive. WinView for...

8/3,K/10 (Item 10 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00040659 DOCUMENT TYPE: Review

PRODUCT NAMES: Simple Network Management Protocol (SNMP) (830056)

TITLE: With SNMP, No LAN Is an Island
AUTHOR: Sprung, Lance
SOURCE: LAN Times, v9 n16 p29(2) Aug 24, 1992
ISSN: 1040-5917
HOMEPAGE: http://www.lantimes.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 940330

...International Standards Organization (ISO) finds network management necessary for fault control, performance, configuration, accounting, and **security** . SNMP is a simple protocol, using only three commands and is **protocol -independent** . An agent, a manager, and a management information base (MIB), along with a command set...
>>>KWIC option is not available in file(s): 278

11/3,K/1 (Item 1 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00087324 DOCUMENT TYPE: Review

PRODUCT NAMES: Common Security Services Manager (CSSM) (596744); Microsoft CryptoAPI (596736); Microsoft Windows 95 (551473); Microsoft Windows 95 (900172); Microsoft Windows NT (347973)

TITLE: Intel, Microsoft creating APIs for encryption
AUTHOR: Moeller, Michael Leach, Norvin
SOURCE: PC Week, v13 n3 p1(2) Jan 22, 1996
ISSN: 0740-1604
HOMEPAGE: http://www.pcweek.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 960530

...beta release of the NT Shell Upgrade release and in a future Windows 95 release. **CryptoAPI** observes the same system-**independent** model as other Windows APIs, and developers write to one interface to call basic functions ...

11/3,K/2 (Item 2 from file: 256)
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00035997 DOCUMENT TYPE: Review

PRODUCT NAMES: Open Systems Interconnection (OSI) (830053)

TITLE: What Are the Standards for Interoperable LAN Security?
AUTHOR: Minoli, Dan
SOURCE: Network Computing, v3 n6 p148(2) Jun 1992
ISSN: 1046-4468
HOMEPAGE: http://www.NetworkComputing.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

REVISION DATE: 980830

...10 standard for data link layer security standards for interoperable LAN security will resolve problems **independent** of the **encryption** algorithm used by devices on LANs. Provisions for authentication, access control, data integrity and confidentiality...

11/3,K/3 (Item 1 from file: 278)
DIALOG(R)File 278:Microcomputer Software Guide

0019304
3089538XX STATUS: ACTIVE ENTRY
TITLE: OnGuard
VERSION: 4.10
RELEASE DATE: 1987
PUBLISHER: United Software Security, Inc.; United SW Security
?
?

```
File   8:Ei Compendex(R) 1970-1998/Dec W2
         (c) 1998 Engineering Info. Inc.
File  77:Conference Papers Index 1973-1998/Nov
         (c) 1998 Cambridge Sci Abs
File 238:Abs. in New Tech & Eng. 1981-1998/Oct
         (c) 1998 Reed-Elsevier (UK) Ltd.
File  35:Dissertation Abstracts Online 1861-1998/Nov
         (c) 1998 UMI
File 202:Information Science Abs. 1966-1998/Sep
         (c)  Information Today, Inc
File  65:Inside Conferences 1993-1998/Nov W5
         (c) 1998 BLDSC all rts. reserv.
File   2:INSPEC 1969-1998/Nov W5
         (c) 1998 Institution of Electrical Engineers
File  94:JICST-EPlus 1985-1998/Sep W1
         (c)1998 Japan Science and Tech Corp(JST)
File 233:Microcomputer Abstracts 1974-1998/Nov
         (c) 1998 Information Today Incl.
File   6:NTIS 64-1998/Dec W4
         Comp&distr 1998 NTIS, Intl Copyright All Righ
File 144:Pascal 1973-1998/Oct
         (c) 1998 INIST/CNRS
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File  99:Wilson Appl. Sci & Tech Abs 1983-1998/Oct
         (c) 1998 The HW Wilson Co.
File 603:Newspaper Abstracts 1984-1988
         (c) 1989 UMI

Set     Items   Description
S1       8283   (INDEPENDENT? OR SEPARATE?)(N2) (LAYER? OR PROTOCOL?)
S2     190796   SECURITY? OR ENCRYPTION? OR DECRYPTION? OR CRYPTO?
S3        107   (SECURE()CHANNEL? OR JAVA(N2)STREAM? OR JAVA()SECURE()CHAN-
              NEL?)
S4      10699   (FIRST AND SECOND)(N2)(NODE? OR PROCESS?)
S5       9790   COMMUNICATION?(N)PROTOCOL?
S6          1   ((COMMUNICATION?)(N2)(CHANNEL? OR PROTOCOL?))(N50)(S2(N3)I-
              NDEPENDENT?)
S7          0   S3 AND S1
S8         29   S1 AND S2
S9          0   S8 AND S5
S10        78   S2 AND S3
S11         7   S10 AND (S1 OR S5)
S12        28   S8 NOT PY=1998
S13        24   RD (unique items)
S14         7   S11 NOT PY=1998
S15         5   RD (unique items)
?
```

6/7/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01232650 E.I. Monthly No: EIM8208-026158
Title: MANAGING DOMAINS IN A NETWORK OPERATING SYSTEM.
Author: Donnelley, J. E.
Corporate Source: Lawrence Livermore Natl Lab, Calif, USA
Conference Title: Local Networks & Distributed Office Systems.
Conference Location: London, Engl Conference Date: 19810500
E.I. Conference No.: 00430
Source: Publ by Online Publ Ltd, Northwood, Engl. Distrib in North Am by Renouf/USA Inc, Brookfield, Vt, USA p 345-361
Publication Year: 1981
ISBN: 0-903796-75-9
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8208

13/7/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04888678 E.I. No: EIP97123955832
Title: Comprehensive multimedia control architecture for the Internet
Author: Schulzrinne, Henning
Corporate Source: Columbia Univ, New York, NY, USA
Conference Title: Proceedings of the 1997 7th International Workshop on Network and Operating System Support for Digital Audio and Video
Conference Location: St.Louis, MO, USA Conference Date: 19970519-19970521
Sponsor: IEEE
E.I. Conference No.: 47528
Source: Proceedings of the IEEE International Workshop on Network and Operating System Support for Digital Audio and Video 1997. IEEE, Piscataway, NJ, USA. p 65-76
Publication Year: 1997
CODEN: 002739
Language: English
Document Type: CA; (Conference Article) Treatment: G; (General Review)
Journal Announcement: 9802W1
Abstract: The Internet and intranets have been used to deliver continuous media, both stored and live, for a number of years. Most of the attention has focused on providing guaranteed quality of service (RSVP) and end-to-end data transport (RTP), with every application using its own control protocol. In this paper, we describe a control architecture that offers most standard advanced telephony features and integrates stored and conference multimedia. The protocol re-uses much of the `infrastructure' of HTTP, including its **security** and proxy mechanisms. The architecture is instantiated by two related, but **independent protocols** : the Session Initiation Protocol (SIP) for inviting participants to a multimedia session and the Real-Time Stream Protocol (RTSP) to control playback and recording for stored continuous media. (Author abstract) 46 Refs.

13/7/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04718197 E.I. No: EIP97063687722
Title: Automated analysis of cryptographic **protocols using Mur phi**
Author: Mitchell, John C.; Mitchell, Mark; Stern, Ulrich
Corporate Source: Stanford Univ, Stanford, CA, USA
Conference Title: Proceedings of the 1997 IEEE Symposium on Security and Privacy
Conference Location: Oakland, CA, USA Conference Date: 19970504-19970507

Sponsor: IEEE
E.I. Conference No.: 46499
Source: Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy 1997. IEEE, Piscataway, NJ, USA,97CB36097. p 141-151
Publication Year: 1997
CODEN: PSSPEO ISSN: 1063-7109
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9707W5
Abstract: A methodology is presented for using a general-purpose state enumeration tool, Mur phi , to analyze **cryptographic** and **security** -related protocols. We illustrate the feasibility of the approach by analyzing the Needham-Schroeder protocol, finding a known bug in a few seconds of computation time, and analyzing variants of Kerberos and the faulty TMN protocol used in another comparative study. The efficiency of Mur phi allows us to examine multiple runs of relatively short protocols, giving us the ability to detect replay attacks, or errors resulting from confusion between independent execution of a **protocol** by **independent** parties. (Author abstract) 19 Refs.

13/7/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04238332 E.I. No: EIP95082834378
Title: Dynamic addressing scheme for wireless media access
Author: Bharghavan, V.
Corporate Source: Univ of California at Berkeley, Berkeley, CA, USA
Conference Title: Proceedings of the 1995 IEEE International Conference on Communications. Part 2 (of 3)
Conference Location: Seattle, WA, USA Conference Date: 19950618-19950622
Sponsor: IEEE
E.I. Conference No.: 43480
Source: IEEE International Conference on Communications v 2 1995. IEEE, Piscataway, NJ, USA,95CH35749. p 756-760
Publication Year: 1995
CODEN: 002115
Language: English
Document Type: CA; (Conference Article) Treatment: A; (Applications); T ; (Theoretical)
Journal Announcement: 9510W4
Abstract: This paper proposes a **protocol independent** Dynamic Addressing scheme for Wireless Media Access Protocols, and discusses related systems and performance issues. Dynamic Addressing allows spatial and temporal reuse of MAC addresses, thereby reducing the address size by a factor of 8. This reduces the control overhead in a MACAW left bracket 2 right bracket style protocol by 30% to 70%, and produces an overall performance improvement of 5% to 33%. Dynamic Addressing also serves as an enabling technology for two important features in wireless media access protocols - **security** , and real-time support - as described in related papers. We are implementing the Dynamic Addressing scheme as a part of the LCMACA wireless media access protocol. (Author abstract) 7 Refs.

13/7/4 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01232650 E.I. Monthly No: EIM8208-026158
Title: MANAGING DOMAINS IN A NETWORK OPERATING SYSTEM.
Author: Donnelley, J. E.
Corporate Source: Lawrence Livermore Natl Lab, Calif, USA
Conference Title: Local Networks & Distributed Office Systems.
Conference Location: London, Engl Conference Date: 19810500
E.I. Conference No.: 00430

Source: Publ by Online Publ Ltd, Northwood, Engl. Distrib in North Am by Renouf/USA Inc, Brookfield, Vt, USA p 345-361
Publication Year: 1981
ISBN: 0-903796-75-9
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8208

13/7/5 (Item 1 from file: 238)
DIALOG(R)File 238:Abs. in New Tech & Eng.

0305595 ANTE NUMBER: 68959
IIOP: the next HTTP?
AUTHOR(S): Clip, P.
JOURNAL: Byte 23 (1) Jan 97 p.47-8. il.
PUBLICATION YEAR: 1997
ISSN: 0360-5280
BLDSC SHELF MARK: 2941.560000
LANGUAGE: English

ABSTRACT: The Internet Inter-ORB Protocol (IIOP), which is part of the Common Object Request Broker Architecture (CORBA), is still a poorly understood protocol. The latest CORBA specification (version 2.1) describes IIOP as the TCP/IP implementation of GIOP, the General Inter-ORB Protocol. GIOP defines a network **protocol -independent** set of messages, formats, and data encoding that all object request brokers (ORBs) must follow when communicating with each other. While GIOP defines the form and content of messages, IIOP encodes the information necessary for invoking methods on objects in IIOP IOR (interoperable object reference) profiles. IOR profiles are composed of a version number, the host and port of the ORB to which messages should be sent, an object key, and a series of components containing information used when invoking methods on the object (eg, the originating ORB's type and **security** parameters). (Abstract quotes from original text)

13/7/6 (Item 1 from file: 35)
DIALOG(R)File 35:Dissertation Abstracts Online

1076287 ORDER NO: AAD89-19869
AN EXTENDED REFERENCE MODEL FOR SUPPORTING INTEGRATED SERVICES COMPUTER COMMUNICATIONS
Author: ALI, MUHAMMAD
Degree: D.SC.
Year: 1989
Corporate Source/Institution: THE GEORGE WASHINGTON UNIVERSITY (0075)
Source: VOLUME 50/06-B OF DISSERTATION ABSTRACTS INTERNATIONAL.
PAGE 2491. 217 PAGES

This study pertains to the design of an extended reference model (ERM) for supporting integrated services computer communications, in an Open Systems Interconnection (OSI) environment. Communications subnetworks for integrated services are coming into use, with a separate control flow for the control of connections carrying user data. However, there is no generally applicable reference model for developing **protocols** supporting **separate** control flows.

The ISO RM supports only "in-band" control for connections and has limitations with regard to OSI management and **security** . Management data flows are pertinent to the OSI environment, but not all components of management flows are supported in the RM. The RM has a definition for **security** services at the seven layers but is deficient in the structural elements that are essential for highly secure computer communications in an OSI environment.

The ISDN Protocol Reference Model (PRM) has architectural and

functional elements for supporting a separate control flow that is fully effective for circuit-switched traffic only. The PRM also has limitations, similar to RM, pertaining to **security** and management flows.

The ERM is designed to overcome these limitations. It is designed as an extension of the ISO Reference Model (RM). An open system of the ERM has five planes that are orthogonal to its seven-layer structure. These planes support the independent-flow (both connection-mode and connectionless-mode) communications supported by the RM. They also support the dependent-flow communications requiring a separate control flow. The ERM has the architectural and functional elements for highly secure communications in the OSI environment and supports all components of the OSI management flows.

The architectural complexity of a software system for independent-flow communication is compared with that of a software system for dependent-flow communication. The former system is based on the ISO RM, and the latter on the ERM. The comparison shows a decrease in architectural complexity when a separate control flow is introduced.

13/7/7 (Item 1 from file: 202)
DIALOG(R)File 202:Information Science Abs.

00216148 9706148
ISA Document Number in Printed Publication: 9706480
It's time for intranets.
Document Type: Journal Article
Author (Affiliation): Zelingher, J. (Ben Gurion Univ., Be'ersheva)
Country of Affiliation: Israel
Journal: M.D. Computing
Publication Language(s): English
Source: Vol. 14 Issue 4 p. 274-275, 277 Jul-Aug 1997

The Internet is a global system of separate computer networks communicating through the Internet protocol, while an intranet is a set of networks operating under one umbrella or one owner--a corporation, government agency, or, in health care, a health maintenance organization or medical center. Access to intranets can be highly regulated and granted only to trusted members of the owner organization. The benefits that intranets offer to smaller healthcare organizations are outlined. These benefits are feasible at the level of a single department or division within any organization, such as a hospital, group practice, or clinic in the ambulatory setting. Use of an intranet in a healthcare facility can be initiated both centrally (by management and information systems personnel) and peripherally (by one or a few functional units.) In addition to offering flexibility and **security** , intranets offer technical benefits. Since the Internet **protocol** is platform-**independent** , intranets can be set up without regard to the type of equipment owned or about to be purchased. Training for end-users is reduced, since standard Web browsers can serve as interfaces on all client stations of the intranet.

13/7/8 (Item 2 from file: 202)
DIALOG(R)File 202:Information Science Abs.

00156265 9106265
ISA Document Number in Printed Publication: 9106232
SAA and NAS: the promise of distributed computing.
Document Type: Journal Article
Author (Affiliation): Rauch, W.
Journal: Data Communications (US)
Publication Language(s): English
Source: p. 68-76 Mar 1991

The author explores the promise of distributed computing: multivendor operability, portability, and scalability with application program interfaces (APIs) and user interface standards. Two distributed

environments, SAA (Systems Application Architecture) and NAS (Network Applications Support) are contrasted relative to IBM versus DEC and their respective technical and marketing orientations. The author presents a feature-by-feature comparison of SAA and NAS, summarized on a Network Services Table which includes the following: **protocol** stack, **protocol -independent** interface, file transfer, directory services, network management, OSI APIs, Gosip, MAP 3.0, distributed file access, remote procedure call, virtual terminal, network **security**, data link control, mainframe communications, PC networking, local-area networking, and wide-area networking.

13/7/9 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

5418010 INSPEC Abstract Number: C9612-7120-019
Title: A framework for building an electronic currency system
Author(s): Lei Tang
Author Affiliation: GSIA, Carnegie Mellon Univ., Pittsburgh, PA, USA
Conference Title: Proceedings of the Sixth Annual USENIX Security Symposium: Focusing on Applications of Cryptography p.113-22
Publisher: USENIX Assoc, Berkeley, CA, USA
Publication Date: 1996 Country of Publication: USA 214 pp.
Material Identity Number: XX96-01392
Conference Title: Proceedings of 6th USENIX UNIX Security Symposium
Conference Date: 22-25 July 1996 Conference Location: San Jose, CA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: We describe a framework for building an electronic currency system. We detail the design of the components of the electronic currency system and the relationships among them. Contrary to previous electronic currency literature, which focuses exclusively on electronic currency protocol designs, we address how to achieve both transaction atomicity and transaction anonymity in the presence of hostile failures, which are common in an electronic currency system if the customers or the merchants are dishonest or malicious. We also propose a recovery method called redo transaction to recover from hostile failures so that the aborted electronic currency transactions caused by the hostile failures can be forced to commit eventually. The structure of the electronic currency system is **protocol -independent** in the sense that the Chaum-like (1981) off-line electronic currency protocol could be incorporated into our framework. (15 Refs)

13/7/10 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

4966671 INSPEC Abstract Number: B9507-6150M-024, C9507-5640-015
Title: Anonymous credit cards of cash and credit cards
Author(s): Low, S.H.; Paul, S.
Author Affiliation: AT&T Bell Labs., Murray Hill, NJ, USA
p.108-17
Publisher: ACM, New York, NY, USA
Publication Date: 1994 Country of Publication: USA x+293 pp.
ISBN: 0 89791 732 4
U.S. Copyright Clearance Center Code: 0 89791 732 4/94/0011.$3.50
Conference Title: Proceedings of 2nd ACM Conference on Computer and Communications Security
Conference Sponsor: ACM
Conference Date: 2-4 Nov. 1994 Conference Location: Fairfax, VA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Applications (A); Practical (P)
Abstract: This paper describes a communications networking technique for

funds transfer which combines the privacy of cash transactions with the **security** , record-keeping and charging mechanisms of credit cards. The scheme uses a communications network and **cryptographic protocols** to **separate** information. The company that extends credit to the individual and collects the bill does not have access to the specific purchases, and the shop that sells the merchandise is convinced that it will be paid without learning the individual's identity. The information is separated to make it difficult to associate an individual with his purchases. Analysis of the information separation in this system shows that five parties must collude to associate an individual's identity and purchases. If an individual deposits cash into the system, rather than asking for credit, then none of the parties need to know his identity. Complete anonymity is obtained while retaining the **security** against loss or theft and the record keeping capabilities of credit cards. (25 Refs)

13/7/11 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

4472785
Title: Databases: more than a bunch of numbers
Author(s): Matheson, K.
Journal: CMA vol.67, no.5 p.13-16
Publication Date: June 1993 Country of Publication: Canada
CODEN: CMAAEA ISSN: 0831-3881
Language: English Document Type: Journal Paper (JP)
Treatment: General, Review (G)
Abstract: Information systems consist of four functional layers: the top layer represents what the user sees; the second layer represents the tools and facilities provided to create applications; the third layer represents the data management functionality; and the fourth layer is the actual data. The value of database systems lies in their ability to manage the four **layers separately** : to manage data because they are important, to provide data to more than one application, to make applications operate on more than one database. An organization should consider five major issues in deciding whether or not to manage data separately from their use in applications: structure, integrity, data sharing, confidentiality and data life cycle. The author discusses all of these points and then discusses client-server information systems. (0 Refs)

13/7/12 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

04031452 INSPEC Abstract Number: C9201-6150J-018
Title: A new look at microkernel-based UNIX operating systems: lessons in performance and compatibility
Author(s): Bricker, A.; Gien, M.; Guillemont, M.; Lipkis, J.; Orr, D.; Rozier, M.
Conference Title: EurOpen. UNIX Distributed Open Systems in Perspective. Proceedings of the Spring 1991 EurOpen Conference p.13-32
Publisher: EurOpen, Buntingford, UK
Publication Date: 1991 Country of Publication: UK viii+331 pp.
Conference Date: 20-24 May 1991 Conference Location: Tromso, Norway
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: With CHORUS V2, the authors experimented with a first-generation microkernel-based UNIX system. UNIX emulation was built as an application of a pure message-based microkernel. Their experience with CHORUS Vs taught them that some functions, such as IPC management, belong within the microkernel. Device drivers and support for heterogeneity, on the other hand, are best handled by **separate** servers and **protocols** . Supervisor actors are crucial to both performance and binary compatibility with existing systems. A global name space is necessary to simplify the

interactions between system servers and the nucleus. Using CHORUS V3, subsystem designers have the freedom to define their operating system architecture and to select the most appropriate tools. Decision, such as the choice between high **security** and high performance, are not to be enforced a priori by the microkernel. The CHORUS V3 microkernel has met its requirements: the CHORUS/MiX microkernel-based UNIX system provides the level of performance of real-time executives, is compatible with UNIX at the binary level, and is truly modular and fully distributed. (12 Refs)

13/7/13 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

03632293 INSPEC Abstract Number: B90039380, C90034592
Title: X.32 function expansion to VENUS-P/LP packet exchange unit
Author(s): Suzuki, T.; Kimura, K.; Shibata, N.
Journal: KDD Technical Journal no.141 p.55-61
Publication Date: July 1989 Country of Publication: Japan
CODEN: KTNKAY ISSN: 0452-3431
Language: Japanese Document Type: Journal Paper (JP)
Treatment: Applications (A); Practical (P)
Abstract: The X.32 function expansion was performed for high speed communication, connection to an international integrated digital communication service, multiple logic channels, improvement of **security** function and replenishment of facilities. The authors discuss the X.32 interface. When introducing the X.32 interface according to the 1988 version CCITT recommendation considerations have been paid to the following: the existing interface must be included because the existing facilities are now providing services; common use with X.28 and X.25 interface and hardware configuration **independent** of the **protocol** . The transmission and reception sequence from an X.32 terminal is illustrated. (5 Refs)

13/7/14 (Item 6 from file: 2)
DIALOG(R)File 2:INSPEC

03564476 INSPEC Abstract Number: B90017551, C90014206
Title: Network security **structure organization based on OSI information network architecture**
Author(s): Dong-Gyu Kim
Journal: Korea Information Science Society Review vol.7, no.5 p. 26-34
Publication Date: 1989 Country of Publication: South Korea
CODEN: CHKWEN
Language: Korean Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Discusses end-to-end **security** system models; prototype **security** systems; porting; formal **security** models; the OSI Protocol Reference Model; peer entity authentication; connection oriented systems; **security** management information base; time stamping; handshaking; data origin authentication; connectionless oriented systems; one-way communication; electronic mail; authentication servers; **encryption** and **decryption** ; eavesdropping; the Data **Encryption** Standard; link **encryption** ; end-to-end **encryption** ; **cryptographic** check-functions; data **security** pipe protocol; asymmetric **cryptographic** public auto-key system; digital signatures; data integrity; padding; notarization; total system management; secure data network systems; **security** protocols; confidentiality; and the Subnetwork **Independent** Convergence **Protocol** . (24 Refs)

13/7/15 (Item 7 from file: 2)
DIALOG(R)File 2:INSPEC

02715373 INSPEC Abstract Number: D86002214

Title: Adopt key management system to keep data networks secure

Journal: Bank Systems & Equipment vol.23, no.4 p.39-40

Publication Date: April 1986 Country of Publication: USA

CODEN: BSEQD6 ISSN: 0146-0900

Language: English Document Type: Journal Paper (JP)

Treatment: General, Review (G)

Abstract: A key management system combines **encryption** and authentication methods to create a safe data network. Electronic distribution of keys is the most efficient means of insuring data **security** . It is important to consider what kind of **encryption** a bank's terminals are capable of, since this will make a difference when the system is expanded in the future. Link **encryption** is done **independently** of the **protocol** and the terminal, so the system is easier to expand than end-to-end **encryption** . (0 Refs)

13/7/16 (Item 1 from file: 233)

DIALOG(R)File 233:Microcomputer Abstracts

00474085 97DM10-003

Managing applications -- Coping with chaos: the fine art of managing enterprise business applications

Foote, Steven

DBMS , October 1, 1997 , v10 n11 p52-62, 6 Page(s)

ISSN: 1041-5173

Reports that the absence of comprehensive solutions for applications management requires IT organizations to piece together best-of-breed products that deliver some level of functionality in one or more of seven management areas. States the products have to deliver functionality in the critical management areas of storage, **security** , event/fault monitoring, and application performance. Adds that users have refined the original definition of applications management to include an application services layer that represents the growing use of middleware in support of distributed application transactions, and a hardware **layer separate** from the operating system layer that represents the latest developments in intelligent hardware components that can be monitored without requiring the operating system to be available. Includes a screen display and a photo. (dpm)

13/7/17 (Item 2 from file: 233)

DIALOG(R)File 233:Microcomputer Abstracts

00450383 97LM02-008

VPNs: just between us -- Here's your confidential guide to everything you ever wanted to know about virtual private networks, including three new up - and - ...

Richardson, Robert

LAN , February 1, 1997 , v12 n2 p99-103, 5 Page(s)

ISSN: 1069-5621

Reports that virtual private networking (VPN) is gaining in popularity because it allows users to outsource remote access points and it offers WAN flexibility. Says that VPN operates on a simple concept: ``you can use the Internet to carry packets where you would otherwise have to use hard wiring to get the job done.'' However, there are unresolved issues relative to standards and network **security** . Reports that two industry initiatives, Point-to-Point Tunneling Protocol and Layer Two Tunneling **Protocol** , **separate** the authorization process from the answering process. Concludes that the greatest impact of VPN is not on cost but ``the strategic implications of how one performs communications with connected communities of interest.'' Includes three diagrams. (phi)

13/7/18 (Item 3 from file: 233)
DIALOG(R)File 233:Microcomputer Abstracts

00390927 95IF07-004
OSI and security analysis: the standard is a valuable blueprint for analyzing complex networks, including non-OSI systems
Holoman, Stuart B
Info Security News , July 1, 1995 , v6 n4 p64-66, 3 Page(s)
ISSN: 1051-2500
Discusses **security** analysis of the Open System Interconnection (OSI) model. Looks at how OSI affects the job of the **security** director, and notes that most **security** lapses can occur in non-required function areas. Presents a detailed look at each of the seven layers of OSI: Layer 1 is a physical layer, a topographical map of the networks, including all wiring; Layer 2 looks at the data-link connection through the error rate history: Layer 3 involves the network, where a map and knowledge of all possible routings is needed; Layer 4 is the transport layer that carries information between the network and end users and it requires its own **separate** routing map; **Layer** 5 is the session layer and requires viewing logon and logoff sequences; Layer 6 is where **encryption** occurs; and Layer 7 is the application layer where **security** involves keeping track of errors and access control. Includes one chart and a sidebar. (eqb)

13/7/19 (Item 4 from file: 233)
DIALOG(R)File 233:Microcomputer Abstracts

00348071 94BY05-007
Agents away -- Telescript is a sophisticated communications language that is the centerpiece of a new style of information network--the electronic...
Wayner, Peter
BYTE , May 1, 1994 , v19 n5 p113-118, 4 Page(s)
ISSN: 0360-5280
Company Name: General Magic
Product Name: Telescript; Magic Cap
Reports on Telescript, an interpreted language from General Magic of Mountain View, CA, which can operate **independently** of all **protocols** and transports. Says that Telescript eases network communication by bundling messages and requests into one query which is transmitted to a distant computer, answered, and returned. Asserts that the language will be especially beneficial to personal digital assistant users. Adds that General Magic also has Magic Cap available, a PDA utility which eases access to phone numbers, addresses, etc. and uses Telescript. Examines the inner workings of Telescript and looks at **security** features. Concludes that while Telescript is limited in access, it is a unique innovation which is a good step forward in network computing. Features a sidebar, ``Speaking the Same Language.'' Includes a diagram and a table. (cnr)

13/7/20 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

2002821 NTIS Accession Number: AD-A321 957/3
Internetworking: Implementation of Multicasting and MBone over Frame Relay Networks
(Master's thesis)
Erdogan, R.
Naval Postgraduate School, Monterey, CA.
Corp. Source Codes: 019895000; 251450
Sep 96 147p
Languages: English Document Type: Thesis
Journal Announcement: GRAI9714
Product reproduced from digital image. Order this product from NTIS by:

phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: PC A08/MF A02

Country of Publication: United States

The major problems addressed by this thesis research are how to implement multicast over the Monterey BayNet to enable live audio/video for distance learning, how to safely integrate regional Frame Relay multicast with the global MBone, and how to monitor multicast connectivity over the Monterey BayNet. To implement multicast and MBone over the Monterey BayNet without using dedicated multicast servers, we enabled **Protocol Independent** Multicast (PIM) **protocol** on already-installed Frame-Relay-capable routers. By implementing multicast over Monterey BayNet, we show that the current MBone software provides the same performance that it provides on regular Internet connections even on low-speed (128Kbps) Frame Relay network connections and low-cost personal computers. In order to control the scope of the regional multicast and to safely integrate regional Frame Relay multicast with the global MBone, we used administratively controlled multicast group addresses (224.0.1.20) in addition to the use of time-to-live (TTL) control mechanism. This eliminates global duplication of multicast packet delivery. Public-domain multicast monitoring tools are used to monitor the multicast connectivity through internetworks. Since these tools are available only to UNIX-based platforms, they cannot be used by the regional sites that mostly have windows and Macintosh platforms. We developed Web-accessible multicast monitoring pages in order to meet the multicast monitoring needs of the regional sites. Participating sites are now able to monitor regional multicast connectivity by accessing these pages, which permits remote problem diagnosis. That was previously impossible. Finally we synopsize firewall requirements for secure and effective use of multicast.

13/7/21 (Item 2 from file: 6)

1956622 NTIS Accession Number: PB96-183165

Distributed Communication Methods and Role-Based Access Control for Use in Health Care Applications

Poole, J. ; Barkley, J. ; Brady, K. ; Cincotta, A. ; Salamon, W.
National Inst. of Standards and Technology (CSL), Gaithersburg, MD.

Corp. Source Codes: 099724000
Report No.: NISTIR-5820
Apr 96 66p
Languages: English
Journal Announcement: GRAI9617

Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: PC A05/MF A01

Country of Publication: United States

The use of software in the health care industry is becoming of increasing importance. One of the major roadblocks to efficient health care is the fact that important information is distributed across many sites. These sites can be located across a significant area. The problem is to provide a uniform mechanism to integrate this information. This paper documents the results of an investigation into the suitability of several different distributed access mechanisms. Five methods were examined; the Common Object Request Broker (CORBA), Object Linking and Embedding (OLE), remote procedure call (RPC), remote database access (SQL/RDA) and **Protocol Independent** Interfaces (PII, the authors specifically examined sockets). These mechanisms were compared with regard for use in health care applications. In particular, the following capabilities were compared: Ease of use by the developer, Class of applications for which the technology is particularly effective in developing, **Security** capabilities.

13/7/22 (Item 3 from file: 6)
DIALOG(R)File 6:NTIS

1420557 NTIS Accession Number: DE89002820
LINCS Authentication Domain Interface (ADI) Logon Protocol: Preliminary Specification and Implementation Guide
Nessett, D. M. ; Fletcher, J. G.
Lawrence Livermore National Lab., CA.
Corp. Source Codes: 068147000; 9513035
Sponsor: Department of Energy, Washington, DC.
Report No.: UCID-30205-REV.1
28 Oct 88 56p
Languages: English
Journal Announcement: GRAI8909; NSA1400
Portions of this document are illegible in microfiche products. Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A04/MF A01
Country of Publication: United States
Contract No.: W-7405-ENG-48
This paper defines the Authentication Domain Interface (ADI) Logon protocol for the LINCS distributed operating system that in conjunction with the Inter-Authentication-Domain Logon protocol gives users of LINCS terminals the ability to logon to hosts that do not support LINCS. In addition, it gives users of terminals connected to networks that do not directly support LINCS the ability to logon and use LINCS distributed resources. Hereafter, for the sake of brevity, the Inter-Authentication-Domain Logon Protocol is called the IAD Logon protocol. The IAD Logon protocol specification describes how the network-level protocols, transport-level protocols, and terminal **protocols** of **separate** authentication domains can be interfaced and defines an inter-authentication-domain logon protocol that supports user authentication and user authorization in the context of multiple authentication domains. The provision of inter-authentication-domain interactive services in LINCS requires interfacing the LINCS network-level, transport-level, virtual terminal, and logon protocols to their corresponding inter-authentication-domain standards through an interactive services gateway. In LINCS, an interactive services gateway is naturally structured as a set of (potentially) distributed modules. This paper describes how a LINCS interactive services gateway can be implemented and describes the actions each of its modules take in the suggested implementation. (ERA citation 14:005722)

13/7/23 (Item 4 from file: 6)
DIALOG(R)File 6:NTIS

0868234 NTIS Accession Number: UCRL-84319(REV.1)/XAB
Resource Access Control in a Network Operating System
Donnelley, J. E. ; Fletcher, J. G.
California Univ., Livermore. Lawrence Livermore Lab.
Corp. Source Codes: 005415009; 9500007
Sponsor: Department of Energy, Washington, DC.
Report No.: CONF-801112-1(REV.1)
1 Aug 80 13p
Languages: English Document Type: Conference proceeding
Journal Announcement: GRAI8106; NSA0500
ACM Pacific 80 conference, San Francisco, CA, USA, 12 Nov 1980.
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.

NTIS Prices: PC A02/MF A01
Country of Publication: United States
Contract No.: W-7405-ENG-48

Computer systems being incorporated into mature support networks are facing a substantial protocol-implementation effort in granting controlled access to their resources and in obtaining access to network-supplied resources. This protocol-implementation effort can be significantly reduced by use of resource-sharing **protocols** that are **independent** of specific resource semantics. A capability-passing model for distributed access control is described and several capability-management protocols are discussed. Highlights of the discussion include the inalienable right to pass capabilities, capability theft through data theft and reflection, capability management by public key **encryption** , a capability passing structure, and resource sharing with integrated network directories. 9 figures, 2 tables. (ERA citation 05:039223)

13/7/24 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1166916 H.W. WILSON RECORD NUMBER: BAST94035509
Agents away
AUGMENTED TITLE: General Magic's Telescript
Wayner, Peter;
Byte v. 19 (May '94) p. 113-14+
DOCUMENT TYPE: Feature Article ISSN: 0360-5280

ABSTRACT: Part of a special section on wireless communications. General Magic's Telescript is an interpreted communications language that works **independently** of all **protocols** and transports. Telescript allows a user to bundle messages, requests, and preferences into an intelligent program that travels to a distant computer, gets answers to all queries, and then brings back the answers. Because of the savings in time, bandwidth, and money provided by Telescript, General Magic sees Telescript as the centerpiece of a global information network. The article describes Telescript and its **security** features and discusses its impending commercial applications.

15/7/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04789479 E.I. No: EIP97083790340
Title: Securing ATM networks
Author: Chuang, Shaw-Cheng
Corporate Source: Univ of Cambridge, Cambridge, UK
Source: Journal of Computer Security v 4 n 4 1996. p 289-329
Publication Year: 1996
CODEN: JCSIET ISSN: 0926-227X
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9710W2

Abstract: In this paper we identify and address the challenges unique to providing a secure ATM network. We analyze the network environment and consider the correct placement of **security** mechanisms, with particular attention to data transfer protection, in such an environment. We then introduce and describe a key agile **cryptographic** device for ATM networks. We present the techniques to provide data confidentiality, synchronization, dynamic key change, dynamic initialization vector change, data integrity and replay protection on ATM data transfer. Finally, we discuss the corresponding control functions for setting up such a **secure channel** . We examine the impact of key exchange protocols on the design of ATM signalling protocols. Our effort in providing novel **security** services in ATM signalling systems has also been presented. (Author abstract) 47 Refs.

15/7/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04546913 E.I. No: EIP96110402160
Title: Calculus for security **bootstrapping in distributed systems**
Author: Maurer, Ueli M.; Schmid, Pierre E.
Corporate Source: ETH Zurich, Zurich, Switz
Source: Journal of Computer Security v 4 n 1 Sep 1996. p 55-80
Publication Year: 1996
CODEN: 002468 ISSN: 0926-227X
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9701W1
Abstract: A calculus of channel **security** properties is presented which allows the analysis and comparison of protocols for establishing **secure channels** in a distributed open system at a high level of abstraction. A channel is characterized by its direction, its time of availability and its **security** properties. **Cryptographic** primitives as well as trust relations are interpreted as transformations for channel **security** properties, and a **cryptographic** protocol can be viewed as a sequence of such transformations. A protocol thus allows to transform a set of **secure channels** established during an initial setup phase, together with a set of insecure channels available during operation of the system, into the set of **secure channels** specified by the **security** requirements. The necessary and sufficient requirements for establishing a **secure channel** between two entities A and B are characterized in terms of **secure channels** to be made available during the initial setup phase and in terms of the minimal trust A and B must have into other entities or into trusted third parties. (Author abstract) 28 Refs.

15/7/3 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

03721468 E.I. No: EIP93101087496
Title: Authenticated datagram protocol: A high performance subtransport level, secure communication protocol
Author: Rangan, P. Venkat
Corporate Source: Univ of California at San Diego, La Jolla, CA, USA
Source: Computers & Security v 12 n 3 May 1993. p 305-314
Publication Year: 1993
CODEN: CPSEDU ISSN: 0167-4048
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9312W1
Abstract: Advances in communication technologies have stimulated the development of computer networks that interconnect competing individuals, organizations, and even countries. In such computer networks, in order to communicate securely, agents must establish **secure channels** to other agents. In this paper, we present a secure **communication protocol** called Authenticated Datagram Protocol (ADP) that establishes host-to-host **secure channels** across networks, and builds agent-to-agent channels on top of host-to-host channels. We show how such a protocol can be layered at the subtransport level of the network protocol hierarchy, so as to provide high performance and **security** even in the presence of untrustworthy entities on the network. (Edited author abstract) 7 Refs.

15/7/4 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

4684953 INSPEC Abstract Number: B9407-6150M-025, C9407-5640-024
Title: Designing secure communication protocols **from trust specifications**

Author(s): Papadimitriou, C.H.; Rangan, V.; Sideri, M.
Author Affiliation: Dept. of Comput. Sci. & Eng., California Univ., San Diego, La Jolla, CA, USA
Journal: Algorithmica vol.11, no.5 p.485-99
Publication Date: May 1994 Country of Publication: West Germany
CODEN: ALGOEJ ISSN: 0178-4617
U.S. Copyright Clearance Center Code: 0178-4617/94/$6.00
Language: English Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: In a very large distributed system, entities may trust and mistrust others with respect to communication **security** in arbitrarily complex ways. We formulate the problem of designing a secure **communication protocol** , given a network interconnection and a ternary relation which captures trust between the entities. We identify several important ways of synthesizing **secure channels** , and study the algorithmic problem of designing a secure **communication protocol** connecting the entities, given the connectivity of the network and the trust relationship between the nodes. We show that whether secure communication is possible can be decided easily in polynomial time. If we also require that channel synthesis proceed along unambiguous paths (in which case the protocol is defined on a spanning tree of the network), we show that the design problem is NP-complete, and we give a linear-time algorithm for an interesting special case of the problem. (4 Refs)

15/7/5 (Item 1 from file: 6)
DIALOG(R)File 6:NTIS

1301185 NTIS Accession Number: AD-A179 326/4
Protocol for Secure Communication in Large Distributed Systems
(Technical rept. 7 Aug 84-6 Aug 87)
Anderson, D. P. ; Ferrari, D. ; Rangan, P. V. ; Sartirana, B.
California Univ., Berkeley. Dept. of Computer Sciences.
Corp. Source Codes: 005029167; 405910
Jan 87 26p
Languages: English
Journal Announcement: GRAI8715
Prepared in cooperation with IBM Corp., Olivetti S.p.A., MICOM-Interlan, Inc., and CSELT S.p.A.
Order this product from NTIS by: phone at 1-800-553-NTIS (U.S. customers); (703)605-6000 (other countries); fax at (703)321-8547; and email at orders@ntis.fedworld.gov. NTIS is located at 5285 Port Royal Road, Springfield, VA, 22161, USA.
NTIS Prices: PC A03/MF A01
Country of Publication: United States
Contract No.: N00039-84-C-0089; ARPA ORDER-4871
A mechanism for secure communication in large distributed systems is proposed. The mechanism, called Authenticated Datagram Protocol (ADP), provides message authentication and, optionally, privacy of data. ADP is a host-to-host datagram protocol, positioned below the transport layer; it uses public-key **encryption** to establish **secure channels** between hosts and to authenticate owners, and single-key **encryption** for communication over a channel and to ensure privacy of the messages. ADP is shown to satisfy the main **security** requirements of large distributed systems, to provide end-to-end **security** in spite of its relatively low level, and to exhibit several advantages over schemes in which **security** mechanisms are at a higher level. The results of a trace-driven measurement study of ADP performance show that its throughput and latency are acceptable even within the limitations of today's technology, provided single-key **encryption** / **decryption** can be done in hardware.
?

File 344:Chinese Patents ABS Apr 1985-1998/Sep
(c) 1998 European Patent Office
File 347:JAPIO Oct 1976-1998/Jul.(UPDATED 981030)
(c) 1998 JPO & JAPIO
File 351:DERWENT WPI 1963-1998/UD=9847;UP=9844;UM=9842
(c)1998 Derwent Info Ltd

Set	Items	Description
S1	12648	(INDEPENDENT? OR SEPARATE?)(N2) (LAYER? OR PROTOCOL?)
S2	38137	SECURITY? OR ENCRYPTION? OR DECRYPTION? OR CRYPTO?
S3	29	(SECURE()CHANNEL? OR JAVA(N2)STREAM? OR JAVA()SECURE()CHANNEL?)
S4	22575	(FIRST AND SECOND)(N2)(NODE? OR PROCESS?)
S5	2324	COMMUNICATION?(N)PROTOCOL?
S6	0	((COMMUNICATION?)(N2)(CHANNEL? OR PROTOCOL?))(N50)(S2(N3)INDEPENDENT?)
S7	0	S3 AND S1
S8	29	S1 AND S2
S9	0	S8 AND S5
S10	19	(INDEPENDENT?) (N4) (ENCRYPTION? OR CRYPTO? OR DECRYPTION?)
S11	0	S10 AND ((COMMUNICATION?) (N2) (PROTOCOL? OR CHANNEL?))
S12	0	S8 AND S5
S13	0	S3 AND S5
S14	47	S1 AND ((COMMUNICATION?) (N2) (PROTOCOL? OR CHANNEL?))
S15	11	S2 AND S3
S16	0	S14 AND S2
S17	1	S4 AND S14
S18	0	S14 AND JAVA
S19	4	S14 AND NODE?
S20	2	S8 NOT SEPARATE?

15/7/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011501812 **Image available**
WPI Acc No: 97-479726/199744
Electronic commerce implementing method especially over public network - governing relationship between customer, merchant and acquirer gateway to perform credit card purchases over network and using secure connection with electronic payment protocol
Patent Assignee: NETSCAPE COMMUNICATIONS CORP (NETS-N)
Inventor: ELGAMAL T
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5671279	A	19970923	US 95555976	A	19951113	H04K-001/00	199744 B

Priority Applications (No Type Date): US 95555976 A 19951113
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
US 5671279	A		24			

Abstract (Basic): US 5671279 A
The method involves using a secure transport layer which includes a channel **security** mechanism comprising a keyed message digest computation. The secure transport layer supports data privacy and integrity for communications between any two network nodes. Two **secure channels** are provided, where ther is one channel between a customer and a merchant and another channel between the merchant and an acquirer gateway, so that the merchant and acquirer are authenticated to each other and to the customer.
A secure courier message is used for implementing an electronic payment protocol that provides at least any of signature, non-repudiation and secondary **encryption** terms. Node-to-node authentication, privacy and data integrity are automatically achieved by the secure transport layer.
USE/ADVANTAGE - E.g. for secure processing of on-line commercial transactions. For credit card payment services, over internet. Uses secure connection in accordance with electronic payment protocol that secures payments and certifies infrastructure that is required to enable all parties to participate in electronic commerce. Provides necessary formats and interfaces between different modules and systems.
Dwg.1/4
Derwent Class: T05; W01
International Patent Class (Main): H04K-001/00

15/7/2 (Item 2 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011457539 **Image available**
WPI Acc No: 97-435446/199740
Secure key replacement in public key cryptography **system - sending key replacement message containing key for decrypting replacement public key and encrypted next replacement key and signing message using both active and replacement public keys**
Patent Assignee: VISA INT SERVICE ASSOC (VISA-N)
Inventor: LEWIS T
Number of Countries: 070 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9731450	A1	19970828	WO 97US2984	A	19970221	H04L-009/08	199740 B
AU 9721377	A	19970910	AU 9721377	A	19970221	H04L-009/08	199802
US 5761306	A	19980602	US 96605427	A	19960222	H04L-009/08	199829
GB 2324449	A	19981021	WO 97US2984	A	19970221	H04L-009/08	199844
			GB 9818207	A	19980820		

Priority Applications (No Type Date): US 96605427 A 19960222
Cited Patents: US 4688250; US 4799258; US 4972472; US 4993067; US 5469507; US 5499294
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 9731450	A1	E	35			
Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN					
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL PT SD SE SZ UG						
AU 9721377	A			Based on		WO 9731450
GB 2324449	A			Based on		WO 9731450

Abstract (Basic): WO 9731450 A

The method of key replacement in an insecure network environment involves generating an active key pair at one node. The pair includes active public and private keys. A replacement key pair is also generated at the node and is encrypted.

The active and encrypted replacement public keys are sent to a second node over a **secure channel** . When the active pair is to be retired, a next replacement key pair is generated at the first node. This new key is encrypted and sent over the channel. The first replacement public key is decrypted at the second node. The first replacement key is then used as the active key. Preferably, the message sent to the second node during the replacement procedure includes the **decryption** key to allow the replacement key to be decrypted.

USE/ADVANTAGE - For secure transaction processing. For automatic teller machine. For bank terminal. For use with personal computer. Robust **encryption** . Requires user to have possession of previous key to use replacement key.

Dwg.1/7

Derwent Class: W01
International Patent Class (Main): H04L-009/08

15/7/3 (Item 3 from file: 351)

DIALOG(R)File 351:DERWENT WPI

011409786 **Image available**
WPI Acc No: 97-387693/199736

System for transferring electronic notes between electronic modules - has processor based electronic modules creating cryptographically secure channel **and transfer and receive electronic notes via channel, each module has memory storing notes with body group of data fields with monetary value data**

Patent Assignee: CITIBANK NA (CITI-N)
Inventor: ROSEN S S
Number of Countries: 017 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 788066	A2	19970806	EP 92119461	A	19921113	G06F-017/60	199736 B
			EP 97105388	A	19921113		

Priority Applications (No Type Date): US 91794112 A 19911115
Cited Patents: No-SR.Pub
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 788066	A2	E	102	Div ex	EP 92119461	
				Div ex		EP 542298
Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE						

Abstract (Basic): EP 788066 A

The system has processor based electronic modules (4-6) which

create a **cryptographically secure channel** and transfer and receive electronic notes via the **secure channel** . Each module has a memory for storing the notes. Each note includes a body group of data fields with data indicative of an initial monetary value of the electronic note.

A transfer group of data fields includes a list of transfer records, each record is generated by a transfer electronic module and has a transferred monetary value and a transferee module identifier. A signature and certificate group of data fields includes a list of transfer devices containing each transfer electronic module's digital signature and certificate.

USE - For implementing electronic money transfers between on-line systems of cooperating banks as alternative medium of economic exchange for cash, cheques, credit and debit cards and electronic funds transfer (EFT).

ADVANTAGE - Allows common payer to payee transactions without intermediation of banking system, and gives control of payment process to individual.

Dwg.1/50

Derwent Class: T01; T05
International Patent Class (Main): G06F-017/60
International Patent Class (Additional): G07F-007/10

15/7/4 (Item 4 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011294471 **Image available**
WPI Acc No: 97-272376/199724

Commercial transaction initiating method enabling seller and buyer to communicate over quasi-public network - receiving seller's message for buyer and transaction and if buyer approves transaction, permits buyer to pay, via agent, for transaction, via secure communication channel using authorisation code

Patent Assignee: FIRST VIRTUAL HOLDINGS INC (FIRS-N)
Inventor: BORENSTEIN N S; LOWERY C M; NEW D; ROSE M T; STEFFERUD E; STEIN L H
Number of Countries: 075 Number of Patents: 004
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9716897	A1	19970509	WO 96US17556	A	19961030	H04K-001/00	199724 B
AU 9675515	A	19970522	AU 9675515	A	19961030	H04K-001/00	199739
US 5757917	A	19980526	US 95548305	A	19951101	H04R-009/00	199828
EP 858697	A1	19980819	EP 96937866	A	19961030	H04K-001/00	199837
			WO 96US17556	A	19961030		

Priority Applications (No Type Date): US 95548305 A 19951101
Cited Patents: 3.Jnl.Ref; US 4799156; US 4947028; US 5283829; US 5291554; US 5329589; US 5420926; US 5557518; US 5590197
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 9716897	A1	E	41			

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

AU 9675515	A		Based on	WO 9716897	
EP 858697	A1	E	Based on	WO 9716897	

Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Abstract (Basic): WO 9716897 A

The method receives a message over the quasi-public network from the seller identifying the buyer and a transaction. A message is

similarly sent to the buyer identifying the transaction. A message is received from the buyer indicating acceptance or refusal of the transaction.

If the buyer's massage indicates approval for the transaction, the seller's agent is communicated with to permit the buyer to pay for the transaction via a secure communication channel. An authorisation code is received from the seller's agent via the **secure channel** . A **cryptographically** signed message is sent including the authorisation code to the seller via the quasi-public network.

USE/ADVANTAGE - E.g. for enabling payment for goods and services over quasi-public network. Enables users of Internet (RTM) to enter into commercial transactions for goods and services.

Dwg.1/9

Derwent Class: T01; W01
International Patent Class (Main): H04K-001/00; H04R-009/00
International Patent Class (Additional): G06F-017/60

15/7/5 (Item 5 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

011042797 **Image available**
WPI Acc No: 97-020721/199702
Clear and secure channels **interface operating - detecting initiation of call being set-up through first and second channels, then sending message in response to initiation of call**
Patent Assignee: MOTOROLA INC (MOTI)
Inventor: KENNEDY P R; SANDBERG T W; WALDRON W B
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5579394	A	19961126	US 94301386	A	19940906	H04N-009/12	199702 B

Priority Applications (No Type Date): US 94301386 A 19940906
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
US 5579394	A		10			

Abstract (Basic): US 5579394 A

The method involves detecting an initiation of a call that is set-up through first and second channels. A message is formed that conveys a signal to initiate a **security** set-up. The initiate **security** set-up signal is at least one audio tone, or an audio voice message. The audio tone is absent from the audio voice message. The message is sent through the first channel, in response to the detecting step. The message conveys an instruction to the second channel to initiate a **security** set-up.

The method further entails determining, after the initiating step, when the **security** set-up signal is received from the first channel. The message is configured to omit the initiate **security** set-up signal from the message. The message is stopped after the initiate **security** set-up signal is received by the second channel.

USE/ADVANTAGE - For establishing secure calls through communication network, for managing and distributing **encryption** keys. Allows reliably starting of secure calls when clear channel cannot be extended between ends of call. Provides compatibility with existing structures of secure terminals.

Dwg.2/5

Derwent Class: W01
International Patent Class (Main): H04N-009/12

15/7/6 (Item 6 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

010988989 **Image available**
WPI Acc No: 96-485938/199648
Transferring electronic money between processor-based electronic modules - transferring electronic notes via cryptographically- secure channel **, each note comprising data fields contg. monetary value, transfer records and sequence number for unique identification of note**
Patent Assignee: CITIBANK NA (CITI-N)
Inventor: ROSEN S S
Number of Countries: 071 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9633476	A2	19961024	WO 96US5521	A	19960419	G07F-007/08	199648 B
AU 9655615	A	19961107	AU 9655615	A	19960419		199709
WO 9633476	A3	19961212					199712
NO 9704835	A	19971219	WO 96US5521	A	19960419	G07F-000/00	199810
			NO 974835	A	19971020		
EP 823105	A1	19980211	EP 96912971	A	19960419		199811
			WO 96US5521	A	19960419		
US 5799087	A	19980825	US 94234461	A	19940428	H04L-009/32	199841
			US 95427287	A	19950421		
CZ 9703323	A3	19980916	WO 96US5521	A	19960419	G07F-007/08	199843
			CZ 973323	A	19960419		
HU 9800982	A2	19980828	WO 96US5521	A	19960419	G07F-007/08	199844
			HU 98982	A	19960419		

Priority Applications (No Type Date): US 95427287 A 19950421; US 94234461 A 19940428
Cited Patents: EP 484603; US 4926325; WO 9116691; WO 9308545; WO 9310503
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 9633476	A2	E	54			
Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN					
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG					
AU 9655615	A			Based on		WO 9633476
EP 823105	A1	E		Based on		WO 9633476
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE						
US 5799087	A			CIP of	US 94234461	
				CIP of		US 5557518
CZ 9703323	A3			Based on		WO 9633476
HU 9800982	A2			Based on		WO 9633476

Abstract (Basic): WO 9633476 A

The electronic note transference system has processor-based electronic modules creating **cryptographically secure channel** and transferring and receiving electronic notes via the channel. Each module has a memory for storing notes.

Each note includes a body group of data indicative of a monetary value, and a transfer group of data fields with a list of transfer records. Each record is generated by a transferor electronic module and includes a sequence number distinguishing a transferred note from other transferred notes transferred from other transferor modules.

USE/ADVANTAGE - For implementing electronic money transactions as alternative medium of economic exchange to cash, cheques, credit and debit cards and electronic funds transfer. Provides enhanced EMS system and elated method for economic exchange that is secure from re-use, duplication and counterfeiting.

Dwg.2/22

Derwent Class: T01; T05
International Patent Class (Main): G07F-000/00; G07F-007/08; H04L-009/32
International Patent Class (Additional): G06F-017/60; G07F-019/00

15/7/7 (Item 7 from file: 351)

DIALOG(R)File 351:DERWENT WPI

009644378
WPI Acc No: 93-337927/199343
Authentication method of terminal user using smartcard - using smartcard encrypted with running value and secret key to provide secure channel **between workstation user and server**
Patent Assignee: INT BUSINESS MACHINES CORP (IBMC)
Inventor: MOLVA R; TSUDIK G
Number of Countries: 004 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 566811	A1	19931027	EP 92810294	A	19920423	G06F-001/00	199343 B
US 5347580	A	19940913	US 9334023	A	19930601	H04L-009/32	199436

Priority Applications (No Type Date): EP 92810294 A 19920423
Cited Patents: 2.Jnl.Ref; EP 140013; EP 234100; US 4679236; WO 8703977
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 566811	A1	E	14			
	Designated States (Regional): DE FR GB					
US 5347580	A		12			

Abstract (Basic): EP 566811 A
The authentication method involves using an authentication server connected to a number of distributed workstations. Each smartcard has a unique identifier and includes a timer, as well as an input and an output with **encryption** via a secret card key. The server has a list of user names, personal identifiers, and at least one secret key.
The workstation receives input data which defines the user, the smartcard and a value derived from the encrypted time. This is encrypted and/or transmitted to the server. The server computes values based on the received data and compares then with other received values. If a match is deemed to have occurred, an accept signal is sent to the workstation.
ADVANTAGE - The smartcard is not personalised and thus is not associated with a partic. user. The secret key of the smartcard is not stored in the authentication server, enabling the processing required for management of the smartcard keys to be minimised.
Dwg.3/5
Abstract (Equivalent): US 5347580 A
The method involves using a smartcard that encrypts the time displayed on the card with a secret, **cryptographically** strong key. The (public)e work station receives as input certain values defining the user, the card and a particular value derived from the encrypted time, and encrypts and/or transmits these values to the server.
The server, in turn, computes from received values some potential values and compares these to other received values. If the server determines a match, an accept signal is transmitted to the work station.
USE - The method involves, e.g. for banking system or data base system.
Dwg.1/5
Derwent Class: T01; T04; T05
International Patent Class (Main): G06F-001/00; H04L-009/32
International Patent Class (Additional): G07F-007/10

15/7/8 (Item 8 from file: 351)
DIALOG(R)File 351:DERWENT WPI

008865482 **Image available**
WPI Acc No: 91-369509/199150
Digital block converting device - converts first block of digital data to second block of digital data
Patent Assignee: ASCOM TECH AG (ASCO-N)

Inventor: LAI X; MASSEY J L
Number of Countries: 016 Number of Patents: 008
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9118459	A	19911128					199150 B
EP 482154	A	19920429	EP 91908542	A	19910516		199218
JP 5500121	W	19930114	JP 91508119	A	19910516	G09C-001/00	199307
			WO 91CH117	A	19910516		
US 5214703	A	19930525	WO 91CH117	A	19910516	H04K-001/04	199322
			US 92781235	A	19920107		
EP 482154	B1	19930630	EP 91908542	A	19910516	H04L-009/06	199326
			WO 91CH117	A	19910516		
DE 59100171	G	19930805	DE 500171	A	19910516	H04L-009/06	199332
			EP 91908542	A	19910516		
			WO 91CH117	A	19910516		
ES 2042346	T3	19931201	EP 91908542	A	19910516	H04L-009/06	199401
WO 9118459	A3	19920305	WO 91CH117	A	19910516		199510

Priority Applications (No Type Date): CH 901690 A 19900518
Cited Patents: No-SR.Pub; EP 221538; US 4255811; NoSR.Pub
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 9118459	A					
Designated States (National): JP US						
Designated States (Regional): AT BE CH DK ES FR GB GR IT LU NL SE						
EP 482154	A	G	39	Based on		WO 9118459
Designated States (Regional): AT CH DE ES FR GB IT LI LU NL SE						
JP 5500121	W			Based on		WO 9118459
US 5214703	A		21	Based on		WO 9118459
EP 482154	B1	G	30	Based on		WO 9118459
Designated States (Regional): AT CH DE ES FR GB IT LI NL SE						
DE 59100171	G			Based on		EP 482154
				Based on		WO 9118459
ES 2042346	T3			Based on		EP 482154

Abstract (Basic): WO 9118459 A

A device (12) for converting a digital block comprises nine coding stages (61.1, 61.2,69) the first eight of which are of identical construction, a coding partial block generation unit (63), an input unit (21) and an output unit (79). Plain text (X) from an information source (11) is coded, blockwise, into coded text (Y) for sending on a transmission line (13), by introducing a secret code block (Z) via a **secure channel** (17).

Four partial blocks (X1-X4,W11-W14,W21-W24,W81-W84,Y1-Y4) are coded in parallel. Each stage (61.1,61.2,69) has four first inputs (25-28,35-38), six or four second inputs (29,30,32,33,49,52;129,130,132,133) and four outputs (75-78).

USE/ADVANTAGE - New, improved block coding which can be brought in line with European Standard. Can also be used to decode cipher text.

(39pp Dwg.No.2/14

Abstract (Equivalent): EP 482154 B

A device (12) for converting a digital block comprises nine coding stages (61.1, 61.2, 69) the first eight of which are of identical construction, a coding partial block generation unit (63), an input unit (21) and an output unit (79). Plain text (X) from an information source (11) is coded, blockwise, into coded text (Y) for sending on a transmission line (13), by introducing a secret code block (Z) via a **secure channel** (17).

Four partial blocks (X1-X4, W11-W14, W21-W24, W81-W84, Y1-Y4) are coded in parallel. Each stage (61.1, 61.2, 69) has four first inputs (25-28, 35-38), six or four second inputs (29, 30, 32, 33, 49, 52; 129, 130, 132, 133) and four outputs (75-78).

USE/ADVANTAGE - New, improved block coding which can be brought in line with European Standard. Can also be used to decode cipher text.

EP-482154 A device for the conversion of in each case a given first digital block of a first length (N) into an associated second binary digital block of equal length (N) with the use of at least one freely

selectable binary control block, characterised by at least one first input (25-26;50,51;125-128) for inputting at least two first subblocks (X1-X4;e1,e2;e5-e8) of a second length (m) which together form the first digital block (X;Wn), by at least one second input (29,30,32,33,49,52,129,130,133) for inputting at least two control blocks (Z1-Z52) of the second length (m), by a logic means (40,60,61.1,61.2,140) which in each case and serially perform at least four logical operations of at least two different kinds (+,.,+), wherein at least the predominants number of all pairs of immediately successive operations consists of two operations of different kinds (+,.,+), wherein by each operation in each case two input blocks (E1,E2) of the second length (m) are converted into an output block (A) of this length (m), wherein first sub-blocks (X1-X4;e1,e2;e5-e8), control blocks (Z1-Z52) and/or output blocks (A) of a respectively preceding operation serve as input blocks (E1,E2), and by at least one output (75-78;47,48;35-38) for outputting at least two second subblocks (Wn1-Wn2,Y1-Y4;a1,a2;a5-a8) of the second length (m) associated with the first sub-blocks (X1-X4;e1,e2;e5-e8) and which together form the second digital block (Wn,Y).

(Dwg.1/14

Abstract (Equivalent): US 5214703 A

The block conversion device comprises nine **encryption** stages (61.1, 61.2, 69), the first eight of which are constructed identically. The conversion device serves for the block-by-block **encryption** of a plaintext (X) proceeding from a message source (11) into a ciphertext (Y) to be delivered on a transmission line (13), in which a secrete key block (Z) is inputted beforehand via a **secure channel** . The **encryption** is effected in a step-by-step and parallel manner for four subblocks (X1-X4; W14;W21-W24; W81-W84; Y1-Y4).

Every **encryption** stage (61.1, 61.2, 69) comprises four first inputs (25-28; 35-38), six and four second inputs (29,30,32,33,49,52; 129,130,132, 133), respectively, and four outputs (75-78). A total of fifty-two key subblocks (Z1-Z52) which are formed from the key block (Z) are connected to the second inputs. The device (12) can also serve, without being altered, for the **decryption** of an incoming ciphertext (Y). Different key subblocks need only be connected to the second inputs for this purpose.

Dwg.2/14

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00; H04K-001/04; H04L-009/06

International Patent Class (Additional): H04L-009/34

15/7/9 (Item 9 from file: 351)

DIALOG(R)File 351:DERWENT WPI

008454958 **Image available**

WPI Acc No: 90-341958/199045

Key management for encrypted packet base networks - involves transmitting call from transparent devices to network from source and balancing traffic through transparent device

Patent Assignee: RACAL DATA COMMUNICATIONS INC (RACA)

Inventor: CAMPBELL T D; TRBOVICH N G

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 4965804	A	19901023	US 89305672	A	19890203		199045 B

Priority Applications (No Type Date): US 89305672 A 19890203

Abstract (Basic): US 4965804 A

In a packet based communication network (10), a key management centre (20) is used to distribute **cryptographic** keys for either a switched virtual circuit or a permanent virtual circuit. The key management centre to communicate directly with the data **encryption** / **decryption** devices (DE's)(14) event though they operate in a

transparent mode (rather than a store and forward mode).
This is accomplished by balancing link counters with calls to fictitious addresses and/or use of interrupt packets transferred between the DET (12) and the DE. In permanent virtual circuits, the MAC of the last packet transmitted under the cold **cryptographic** key is exchanged to synchronise the key change.
ADVANTAGE - Conforms to current standards while requiring no dedicated **secure channel** . (15pp Dwg.No.1/5)
Derwent Class: W01
International Patent Class (Additional): H04L-009/00

15/7/10 (Item 10 from file: 351)
DIALOG(R)File 351:DERWENT WPI

004377949
WPI Acc No: 85-204827/198534
Multi-channel broadcasting system - transmits encryption **and decoding signals over** secure channel **then stores and cancels after use**
Patent Assignee: COMMUNICATIONS PATENTS LTD (COMZ)
Inventor: BAKER H L
Number of Countries: 011 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 152251	A	19850821	EP 85300728	A	19850204		198534 B
GB 2154108	A	19850829	GB 852750	A	19850204		198535
AU 8538450	A	19850815					198540
JP 60248043	A	19851207	JP 8520995	A	19850207		198604
GB 2154108	B	19870603					198722
CA 1236885	A	19880517					198824

Priority Applications (No Type Date): GB 843164 A 19840207
Cited Patents: 1.Jnl.Ref; A3...8631; EP 93549; EP 94794; No-SR.Pub; US 4045814
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 152251	A	E	12			

Designated States (Regional): BE CH DE FR GB LI NL SE

Abstract (Basic): EP 152251 A
The system has a signal distribution network for transmitting signals on a number of channels between a head end and subscriber terminals. A channel selector switch for each terminal in controllable by the subscriber to select the channel on which to receive signals. Data signals are encrypted and transmitted over at least one channel. Set(s of **encryption** and **decryption** signals are generated by a circuit remote from the terminals. Either the **encryption** or **decryption** signals of one set are transmitted on a predetermined second channel to the terminal. A switch is controlled to temporarily select the second channel to receive the signals and then switched back to the first channel.
The data signal is encrypted at the source by stored signals and decrypted at the destination using stored **decryption** signals.
USE/ADVANTAGE - For e.g. conducting banking operations. Enciphering Enciphering/deciphering codes are not generally available to subscribers and can be changed each time transaction ins carried out or whenever **security** demands.
0/1
Abstract (Equivalent): GB 2154108 B
A broadcasting system comprising a head end, a plurality of subscriber terminals, a signal distribution network for transmitting signals on a plurality of channels between the head end and the subscriber terminals, a channel selector switch in respect of each terminal controllable by the subscriber to select the channel on which it is desired to receive signals, and means for encrypting data signals and transmitting the encrypted data signals over at least one channel

of the network, the data signal encrypting and transmitting means comprsiing means remote from the subscriber terminals for generating at least one set of **encryption** and **decryption** information signals to be used in encrypting and decrypting the data signals to be transmitted over the one channel, means for transmitting either the **encryption** or the **decryption** information signals of said one set on a predetermined other channel to the one terminal, the predetermined other channel not being accessible to any terminal by operation of the terminal selector switch by the subscriber, means for controlling the terminal selector switch of the one terminal temporarily to select the predetermined other channel and then switch back to the one channel, whereby the transmitted **encryption** or **decryption** information signals are received by the one terminal only, means for storing the **encryption** and **decryption** information signals at the source and destination respectively of the data signal to be transmitted, and means for encrypting the data signal at the source using the stored encrypted data signal to the destination over the one channel, and decrypting the encrypted data signal at the destination using the stored **decryption** information signals.

Derwent Class: P85; W01; W02
International Patent Class (Additional): G09C-001/00; H04H-001/02; H04K-001/00; H04L-009/00; H04N-007/16

15/7/11 (Item 11 from file: 351)
DIALOG(R)File 351:DERWENT WPI

001307131
WPI Acc No: 75-K1052W/197537
Secure channel **selection in time multiplexed data transmission - ensures that receiver switches channels correctly using highly redundant code**
Patent Assignee: SIEMENS AG (SIEI)
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 1591566	B	19750904					197537 B

Priority Applications (No Type Date): DE 1591566 A 19670929

Abstract (Basic): DE 1591566 B
An encoding format for time multiplexed data transmission is presented in which the channels at the receiving end are provided with the correct information with a very high degree of **security** .
This is achieved by using a highly redundant encoding system incorporating a channel address with each transmitted data bit. The system is illustrated by considering an eight channel time multiplexed system transmitting data at 50 Bauds in each channel.
Each data bit lasts therefore 20 ms. The multiplexer however scans the channels at 2400 Hz, thus transmitting six bits of information for every channel bit of information. These six bits are transmitted in series, with the eight channels interlaced at 2400 Hz. The six bits consist of a start bit, three bits representing the channel address, the information bit and a stop bit
Derwent Class: W02
International Patent Class (Additional): H04J-003/06

17/7/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011525609 **Image available**
WPI Acc No: 97-502095/199746
Method of accessing unique features of telephony network using protocol independent **interface for e.g video conferencing system - involves establishing telephony by connection-oriented telephony network between**

first and second computers, and transmitting data streams between first process **on** first **computer and** second process **on** second **computer**
Patent Assignee: ANDERSEN D B (ANDE-I); TAI T C (TAIT-I)
Inventor: ANDERSEN D B; TAI T C
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5674003	A	19971007	US 95430460	A	19950428	G06F-017/00	199746 B

Priority Applications (No Type Date): US 95430460 A 19950428
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
US 5674003	A		16			

Abstract (Basic): US 5674003 A

The method involves creating a first socket group comprising a first number of socket communication endpoints for use by the at least one **first** computer **process** on the **first** computer. A required quality-of-service associated with the first socket group is determined. A telephony connection is established by the connection-oriented telephony network between the first and second computers. A second socket group is created which includes a second number of socket communication endpoints for use by the second computer.

A number of **communication channels** are established between each of the first number of sockets and corresponding ones of the second number of sockets. A number of data streams are transmitted between the **first process** on the **first** computer and the **second process** on the **second** computer by the number of **communication channels** multiplexed on the telephony connection.

ADVANTAGE - Exploits characteristic of telephony network not available or not required in connectionless network such as LAN and WAN.

Dwg.1/5
Derwent Class: T01; W01
International Patent Class (Main): G06F-017/00

19/7/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

010845532 **Image available**
WPI Acc No: 96-342485/199634
Packet radio mobile communications system - encapsulates data packets of external data network using point to point protocol and passes them through sub networks to point which supports protocol
Patent Assignee: NOKIA TELECOM OY (OYNO)
Inventor: HAMALAINEN J; KARI H H; KARPPANEN A; HAEMAELAEINEN J; AHOPELTO J
Number of Countries: 071 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9621984	A2	19960718	WO 96FI20	A	19960108	H04L-012/56	199634 B
FI 9500117	A	19960711	FI 95117	A	19950110	H04L-029/06	199641
AU 9643929	A	19960731	AU 9643929	A	19960108	H04L-012/56	199645
WO 9621984	A3	19960912	WO 96FI20	A	19960108	H04L-012/56	199645
FI 98027	B	19961213	FI 95117	A	19950110	H04L-029/06	199704
NO 9703177	A	19970909	WO 96FI20	A	19960108	H04L-012/56	199747
			NO 973177	A	19970709		
EP 804845	A1	19971105	EP 96900337	A	19960108	H04L-012/56	199749
			WO 96FI20	A	19960108		

Priority Applications (No Type Date): FI 95117 A 19950110
Cited Patents: US 4755992; US 5446736; WO 9600468; No-SR.Pub
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 9621984	A2	E	27			

Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE

DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN
Designated States (Regional): AT BE CH DE DK EA ES FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

AU 9643929	A	Based on	WO 9621984	
FI 98027	B	Previous Publ.	FI 9500117	
EP 804845	A1 E	Based on	WO 9621984	

Designated States (Regional): AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

Abstract (Basic): WO 9621984 A

The packet radio mobile communication network uses a point-to-point **protocol independent** of the universal **communication protocol** in the internal transmission of the packet radio system. A data packet according to the protocol contains the control fields used by the protocol, an identification field identifies the protocol used by the terminal equipment and a data field. A data packet according to the universal protocol is thus encapsulated in the data field of a data packet according to the point to point protocol in the internal transmission of the packet radio system. A special radio link protocol is used between the packet data terminal equipment and the packet radio support **node** on the radio interface. The radio link protocol supports point-to-multipoint addressing and the control of data packet retransmission. A data packet according to the radio link protocol contains the control fields used by the protocol and a data field.

The packet data terminal and the support **node** are arranged to compress a data packet according to the point-to-point protocol transmitted over the radio interface by removing at least one control field and to encapsulate the remaining fields in the data field of a data packet according to the radio link protocol. The packet data terminal and support **node** are arranged to decompress received data according to the protocol, by adding the fields previously removed.

USE/ADVANTAGE - Supports several external data networks and protocols enabling new protocols to be supported as flexibly as possible and with only minor modifications.

Dwg.4/4

Derwent Class: W01
International Patent Class (Main): H04L-012/56; H04L-029/06
International Patent Class (Additional): H04L-012/66

19/7/2 (Item 2 from file: 351)
DIALOG(R)File 351:DERWENT WPI

007541681 **Image available**
WPI Acc No: 88-175613/198825

I-O network for computer system - provides data communication between several widely dispersed devices interconnected by LAN type media using processor at each node

Patent Assignee: DATAPOINT CORP (DATA-N)
Inventor: FISCHER M A; FISHER M A
Number of Countries: 020 Number of Patents: 012
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 8804511	A	19880616	WO 87US2388	A	19870918		198825 B
AU 8780394	A	19880630					198838
NO 8803578	A	19881128					198902
DK 8804449	A	19880920					198904
EP 333715	A	19890927	EP 87906709	A	19870918		198939
JP 2501787	W	19900614					199030
US 4941089	A	19900710	US 86941084	A	19861212		199030
CA 1293820	C	19911231					199208
EP 333715	B1	19931201	EP 87906702	A	19870918	H04Q-009/00	199348
			WO 87US2388	A	19870918		
DE 3788355	G	19940113	DE 3788355	A	19870918	H04Q-009/00	199403
			EP 87906702	A	19870918		

			WO 87US2388	A	19870918			
NO 174910	B	19940418	WO 87US2388	A	19870918	H04Q-009/00		199419
			NO 883578	A	19880812			
EP 333715	A4	19910131	EP 87906702	A	19870000			199515

Priority Applications (No Type Date): US 86941084 A 19861212
Cited Patents: US 4423414; US 4495493; US 4549297; US 4574284; US 4680581; US 4692918; US 4706080; No-Citns.
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
WO 8804511	A	E	93			
				Designated States (National): AU BR DK FI JP KP NO		
				Designated States (Regional): AT BE CH DE FR GB IT LU NL SE		
EP 333715	A	E				
				Designated States (Regional): AT BE CH DE FR GB IT LU NL SE		
EP 333715	B1	E	33	Based on		WO 8804511
				Designated States (Regional): AT BE CH DE FR GB IT LI LU NL SE		
DE 3788355	G			Based on		EP 333715
				Based on		WO 8804511
NO 174910	B			Previous Publ.		NO 8803578

Abstract (Basic): WO 8804511 A

The I/D network channel has a network communication medium for extending over a large physical distance. An interface connects each individual computer system device to a separate connection point on the medium. Each interface device has a predetermined ID number which distinguishes each **node** .

A data transmitter is controlled to transmit link level information as part of each data message and to transmit physical level communication information which identifies the transmission of each data message. The controller responds to the transmitted information to cause the buffer to hold only those data messages having destination information specifying the partic. **node** .

ADVANTAGE - Efficient time sharing of computer system resources, high data communication rate

Abstract (Equivalent): EP 333715 B

A system to implement A character I/O channel (140: 140a, 140b) for communicating byte stream data (266) and control administrative information (264) in single IONET network level data packet messages (240) from source to destination Devices connected to the channel (140; 140a, 140b) at a plurality of **Nodes** (174), each Device including a device interface (182) which connects to a device (176, 100; 176a, 100a, 100b) which is separate from the Device, the device (176, 100; 176a, 100a, 100b) being one of either an I/O device (176; 176a) which conducts I/O data transfers or a computer device 9100; 100a, 100b) including a memory (104) and a processor means (102) and a program code for operating the computer device (100; 100a, 100b), said character I/O channel (140; 140a, 140b) being for use in conjunction with a local area network (LAN) comprising a communication medium (170; 170a, 170b) commonly connecting the plurality of **Nodes** (174), LAN interface means (178) at each **Node** (174) for controlling access to the medium (170; 170a, 170b) and communicating LAN packets between predetermined selected source and destination **Nodes** (174), each LAN data packet including a LAN data field and a LAN header field containing characterise which controls the interface means (178) to achieve **Node** to **Node** communications in accordance with a predetermined LAN **communication protocol** , characterised in that said character I/O channel (140; 140a, 140b) comprises in combination: point of use (POU) means (172) included in the Device and connected to the LAN interface means (178) at each **Node** (174), the POU means (172) connected to each I/O device (176; 176a) including a microcomputer means (180) including a memory and a program code for operating the microcomputer means (180); the program codes for the processor means (102) and the microcomputer means (180) defining a predetermined IONET **communication protocol** for communicating with Devices and their connected device interface (182) and devices (176, 100; 176a, 100a, 100b), the IONET **communication protocol** being **separate** from the LAN **communication protocol** , the POU means (172) being adapted to insert chambers in the

data field of LAN data packets to form the IONET network level data packet messages (240) which have an IONET header field (260) and an administrative field (264) and a byte stream data field (266), the IONET header characterise (260) including a function code (278) specifying one of a plurality of control functions, the administrative field characters including an administrative information code (264) for use in accomplishing the specified control function to be performed by one of the Device or its device interface (182), the byte stream data characters (266) originating from a device (176, 100; 176a, 100a, 100b) at the source **Node** (174), and the POU means (172) of the destination **Node** (174) being adapted to directly interpret the function code (278) and the administrative information code characters (264) (a) to establish a session between the source and destination Devices to communicating IONET data packet messages (240) therebetween without acceptance of and interference from other IONET data packet messages (240) for the duration of the session, and (b) to perform a corresponding control function on one of the destination Device or its device interface (182) during the session, and (c) simultaneously to transfer to byte stream data characters (266) in unmodified form directly to the device (176, 100; 176a, 100a, 100b) connected to the device interface (182) of the destination Device.

(Dwg.2/18

Abstract (Equivalent): US 4941089 A

The IONET channel allows highly effective character and other communication between a number of low and medium speed devices of the same or mixed types connected directly to the I/O subsystem of a computer system.

By using arbitration over LAN-type communication medium, relatively low cost point of use adapters with microcomputers distributed over the medium and connected to each I/O device individually or to a relatively small number of I/O devices are possible. A **communication** and control **protocol** efficiently controls the microcomputers and controls communication of the data between the I/O devices and the computer system memory.

The LAN-type **communication** medium, the **protocol** and the distributed low cost point of use adapters cooperatively function as an improved I/O channel controller. USE/ADVANTAGE - I/O network (IONET) channel for a computer system.

Efficient and reduced cost.

(36pp

Derwent Class: T01; W01
International Patent Class (Main): H04Q-009/00
International Patent Class (Additional): G06F-013/00; H04J-003/24; H04J-006/00; H04L-012/40; H04L-029/06

19/7/3 (Item 3 from file: 351)
DIALOG(R)File 351:DERWENT WPI

007130776
WPI Acc No: 87-130773/198719
Communication system for digital message block transfer - uses single communication channel **for transmission of both small and large message blocks utilising polling priority scheme**
Patent Assignee: MINNESOTA MINING & MFG CO (MINN)
Inventor: NELSON O L; RENNOLET C L
Number of Countries: 010 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 221708	A	19870513	EP 86308078	A	19861017		198719 B
JP 62100044	A	19870509	JP 86246462	A	19861016		198724
US 4763323	A	19880809	US 87129386	A	19871124		198834
CA 1263721	A	19891205					199002
EP 221708	B1	19920708	EP 86308078	A	19861017	H04L-012/40	199228
DE 3685935	G	19920813	DE 3685935	A	19861017	H04L-012/40	199234
			EP 86308078	A	19861017		

Priority Applications (No Type Date): US 85789093 A 19851018
Cited Patents: 1.Jnl.Ref; A3...8906; JP 59211352; No-SR.Pub; US 3702008; US 4177450; US 4340961
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
EP 221708	A	E	40			
Designated States (Regional): BE DE FR GB IT NL SE						
US 4763323	A		15			
EP 221708	B1	E	23			
Designated States (Regional): BE DE FR GB IT NL SE						
DE 3685935	G			Based on		EP 221708

Abstract (Basic): EP 221708 A

Nodes (26,28,30,32,34,36) are coupled to a common wideband **communication channel** (12) for the transfer of small and large digital message blocks. One of the **nodes** (26-36) is a master mode controlling the **communication** on the **channel** (12) by selectively polling the other **nodes** (26-36). The system (10) has two **separate protocols** for the transmission of small and large message blocks.

The master **node** establishes a polling priority (66) for each **node** and polls those with a higher polling priority more frequently than those with a lower priority. The master **node** allows the one **node** being polled to communicate over the channel (12) of either a small or a large digital message block. The master **node** adapts the polling priority (66) for each **node** based upon a predetermined algorithm.

Abstract (Equivalent): EP 221708 B

A communication system (10) for the transfer of small digital message blocks and large digital message blocks, having: a common **communication channel** (12) capable of facilitating the transfer of small digital message blocks and large digital message blocks; a plurality of **nodes** (26-36) coupled to said channel, each being capable of communicating over said channel and each adapted to be coupled to a digital handling device (14-24); one of said plurality of **nodes** being designated as a master **node** , said master **node** controlling communcation on said channel by selectively polling the other of said plurality of **nodes** , said master **node** establishing a polling priority (66) for each of said plurality of **nodes** and polling those of said plurality of **nodes** with a higher of said polling priority more frequently than those of said plurality of **nodes** with a lower of said polling polarity; said master **node** allowing the one of said plurality of which is being polled to communicate over said channel with either said small digital message block or said large digital message block, characterized in that said communication system has a first protocol for the transmission of said small digital message blocks in a short time frame and has a second protocol for the transmission of said large digital message blocks in a long time frame, said long time frames being at least two orders of magnitude greater than said short time frames; said master **node** adapting said polling priority for each of said plurality of **nodes** based upon a predetermined algorithm; and wherein said master **node** adapts said polling priority for each of said plurality of **nodes** based upon whether a given **node** has recently had a digital message communication and based upon whether such digital message communication was a small digital message block or a large digital message block. (Dwg.5/8)N

Abstract (Equivalent): US 4763323 A

Nodes are coupled to a common wideband **communication channel** capable of facilitating the transfer of small and large digital message blocks. One of the **nodes** is a master **node** controlling the communication of the **communication channel** by selectively polling the other **nodes** .

The communication system has a first protocol for the transmission of small digital message blocks and a second protocol for the transmission of large ones. The master **node** establishes a polling priority for each **node** and polls those with a higher polling priority more frequently than those with a lower polling priority. The master

node allows the one **node** being polled to communicate over the channel of either a small or large digital message block. Further, the master **node** adapts the polling priority for each of the **nodes** based upon a predetermined algorithm.

Derwent Class: W01
International Patent Class (Main): H04L-012/40
International Patent Class (Additional): H04J-003/16; H04L-011/16

19/7/4 (Item 4 from file: 351)
DIALOG(R)File 351:DERWENT WPI

003277108
WPI Acc No: 82-C5092E/198209
Transparent intelligent network for data and voice - operates independently **of customer** protocol **and enables** communication **via central unit in limited stages**
Patent Assignee: TEXAS INSTR INC (TEXI)
Inventor: ULUG M E
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 4316283	A	19820216					198209 B

Priority Applications (No Type Date): US 80139914 A 19800414; US 78912116 A 19780602
Patent Details:

Patent	Kind	Lan	Pg	Filing Notes	Application	Patent
US 4316283	A		26			

Abstract (Basic): US 4316283 A

In a situation where connection is made to an X-25 computer and to a polled line, the network strips off the user protocol and only transmits that part of the information which represents usable data to the polled line. When the transmission is received back from the output port, appropriate protocol is reinserted, and it therefore appears to the external connections as if they are directly connected to each other.

A system of the 2-level hierarchial type has a number of near neighbour connected star nets each having a central **node** . The central **nodes** are each directly connected to each other via 12-14 GHz satellite channels as well as terrestrial links which carry mostly protocol messages and re-transmissions for the purposes of error correction, although some part or all of the real time traffic can also be sent over the terrestrial links. This assures no more than three transmission hops between point of entry and destination, and contributes to speed and accuracy of transmission.

Derwent Class: T01; W02
International Patent Class (Additional): H04J-006/00

20/7/1 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011459905 **Image available**
WPI Acc No: 97-437812/199741
Information transmission method in cellular mobile network - indicating frame number of transmission frame, maintaining function of secured information transmission for subscriber or network device
Patent Assignee: SIEMENS AG (SIEI)
Inventor: NIEPEL H; ROESLER O
Number of Countries: 005 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 794679	A2	19970910	EP 97103469	A	19970303	H04Q-007/22	199741 B

Priority Applications (No Type Date): DE 1008205 A 19960304
Cited Patents: No-SR.Pub
Patent Details:
Patent Kind Lan Pg Filing Notes Application Patent
EP 794679 A2 G 8
Designated States (Regional): DE ES FR GB IT

Abstract (Basic): EP 794679 A
The formation or disconnection of an information securing connection of a subscriber device or a network device is initialised or acknowledged in the coupling field of a transmission frame. Renewal characters are input to indicate a frame number of a numbered transmission frame. The renewal characters are used to determine whether a frame is transmitted before or after formation or disconnection of a connection.
The function of the secured information transmission is maintained. A transmission variable is set to a start value for the numbering of the frames to be transmitted according to the renewal characters. The transmission variable is used to determine the frame number of the next numbered transmission frame to be transmitted in sequence.
ADVANTAGE - Maintains **security protocol independently** of physical structure of logical function channel.
Dwg.2/2
Derwent Class: W01; W02
International Patent Class (Main): H04Q-007/22

20/7/2 (Item 2 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

007072469
WPI Acc No: 87-072466/198710
Monitoring status of security **devices - using non-interfering in-band** protocol- independent **diagnostic scanning in digital multipoint communication system**
Patent Assignee: PARADYNE CORP (PDYN)
Inventor: ARMSTRONG T; BREMER G; HOLMQUIST K; SMITH R K
Number of Countries: 001 Number of Patents: 001
Patent Family:
Patent No Kind Date Applicat No Kind Date Main IPC Week
US 4645871 A 19870224 US 85745849 A 19850617 198710 B

Priority Applications (No Type Date): US 85745849 A 19850617
Patent Details:
Patent Kind Lan Pg Filing Notes Application Patent
US 4645871 A 7

Abstract (Basic): US 4645871 A
The **security** status encoder (25) comprises a DES encryptor operated in the K-bit cipher feedback mode. The DEE (12) comprises an automatic switch (30), a DES encoder (32) and a remote I
3/4
Derwent Class: T05; W01
International Patent Class (Additional): G07D-007/00; G08B-005/22; H04L-009/00

10/3,K/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 1998 JPO & JAPIO. All rts. reserv.

03599327
SECRECY COMMUNICATION SYSTEM

PUB. NO.: 03-262227 [JP 3262227 A]
PUBLISHED: November 21, 1991 (19911121)
INVENTOR(s): ICHIYOSHI OSAMU

APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 02-060110 [JP 9060110]
FILED: March 13, 1990 (19900313)
JOURNAL: Section: E, Section No. 1168, Vol. 16, No. 67, Pg. 143, February 19, 1992 (19920219)

ABSTRACT

...CONSTITUTION: Identification/cryptographic memories 32, 37 storing lots of the personal identification codes and **cryptographic** codes **independently** of the lots of personal identification codes in same addresses are provided on both communication...

10/3,K/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO
(c) 1998 JPO & JAPIO. All rts. reserv.

02486633
CRYPTOGRAPHIC COMMUNICATION PROCESSING SYSTEM

PUB. NO.: 63-103533 [JP 63103533 A]
PUBLISHED: May 09, 1988 (19880509)
INVENTOR(s): MATSUNAGA HIROSHI
APPLICANT(s): MITSUBISHI ELECTRIC CORP [000601] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 61-249214 [JP 86249214]
FILED: October 20, 1986 (19861020)
JOURNAL: Section: E, Section No. 658, Vol. 12, No. 342, Pg. 117, September 14, 1988 (19880914)

ABSTRACT

... interface to a data input/output device so as to eliminate the need for an **independent** **cryptographic** communication equipment and a cryptographic key input device...

10/3,K/3 (Item 1 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

011742852 **Image available**
WPI Acc No: 98-159762/199814
XRPX Acc No: N98-126919
Ternary cascadable content addressable memory device for coupling to external device - has memory cells forming multiple bit storage words for storing ternary data, and addressable mask register subsystem for binary-ternary data conversion options selection
Patent Assignee: BELL COMMUNICATIONS RES INC (BELL-N); MOTOROLA INC (MOTI)
Inventor: KEMPKE R A; MCAULEY A J
Number of Countries: 070 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9807160	A2	19980219	WO 97US13216	A	19970729	G11C-011/56	199814 B
AU 9738162	A	19980306	AU 9738162	A	19970729	G11C-011/56	199830

Priority Applications (No Type Date): US 96696453 A 19960813
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
WO 9807160	A2			

Designated States (National): AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE HU IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG UZ VN
Designated States (Regional): AT BE CH DE DK ES FI FR GB GR IE IT LU MC NL PT SE

AU 9738162 A Based on WO 9807160
Language, Pages: WO 9807160 (E, 35)

...Abstract (Basic): ADVANTAGE - Utilises off-loaded key **encryption** of pay loads, **independent** of address routing information e.g. VP1/VC1...

10/3,K/4 (Item 2 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011591135 **Image available**
WPI Acc No: 98-008264/199801
XRPX Acc No: N98-006561
Cryptography system to support application requiring cryptographic function - uses private application program interface to interface cryptography service provider with user
Patent Assignee: MICROSOFT CORP (MICR-N)
Inventor: SIMON D R; SPELMAN J F; SPIES T R
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5689565	A	19971118	US 95496801	A	19950629	H04L-009/00	199801 B

Priority Applications (No Type Date): US 95496801 A 19950629
Language, Pages: US 5689565 (41)

...Abstract (Basic): interface with the application and handle its requests for a cryptographic function. At least one **cryptography** service provider (CSP) **independent** from. but dynamically is accessible by the CAPI. The CSP provides the cryptographic function requested...

10/3,K/5 (Item 3 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011385364 **Image available**
WPI Acc No: 97-363271/199733
XRPX Acc No: N97-302080
Method of controlling access to subset of items of digital information in high-capacity storage media e.g CD-ROM - involves providing decryption key which permits decryption of items belonging to arbitrarily selected subset of items, encryption keys are associated with corresponding decryption keys
Patent Assignee: DIGITAL DELIVERY INC (DIGI-N)
Inventor: HASTINGS T M; SUBLER R J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5646992	A	19970708	US 93126217	A	19930923		199733 B

Priority Applications (No Type Date): US 93126217 A 19930923
Language, Pages: US 5646992 (25)

...Abstract (Basic): keys are encrypted using a single global encryption key. The global decryption key being the **decryption** key which is **independent** of the composition of the arbitrarily selected subset. a request for access to the items...

10/3,K/6 (Item 4 from file: 351)
DIALOG(R)File 351:DERWENT WPI

011074672 **Image available**
WPI Acc No: 97-052596/199705

XRPX Acc No: N97-043089
Public key cryptography independent **electronic cash transfer for off-line cash system - involves storing electronic record of electronic coin withdrawn by user and payed to payee to determine validity of coin**
Patent Assignee: BRICKELL E F (BRIC-I); GEMMELL P S (GEMM-I); KRAVITZ D W (KRAV-I)
Inventor: BRICKELL E F; GEMMELL P S; KRAVITZ D W
Number of Countries: 070 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
WO 9641316	A2	19961219	WO 96US10247	A	19960607	G07F-019/00	199705 B
AU 9667613	A	19961230	AU 9667613	A	19960607	G07F-019/00	199716
WO 9641316	A3	19970306	WO 96US10247	A	19960607	G07F-019/00	199728

Priority Applications (No Type Date): US 95482686 A 19950607; US 95474033 A 19950607; US 95474035 A 19950607; US 95482356 A 19950607; US 95482685 A 19950607
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
WO 9641316	A2			

Designated States (National): AL AM AT AU AZ BB BG BR BY CA CH CN CZ DE DK EE ES FI GB GE HU IS JP KE KG KP KR KZ LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK TJ TM TR TT UA UG US UZ VN
Designated States (Regional): AT BE CH DE DK EA ES FI FR GB GR IE IT KE LS LU MC MW NL OA PT SD SE SZ UG

AU 9667613	A	Based on	WO 9641316

Language, Pages: WO 9641316 (E, 97)

Public key cryptography independent **electronic cash transfer for off-line cash system...**

10/3,K/7 (Item 5 from file: 351)
DIALOG(R)File 351:DERWENT WPI

010013797 **Image available**
WPI Acc No: 94-281508/199435
XRPX Acc No: N94-221902
High-speed encryption system using multiple key-stream generator - uses linear feedback shift register that supplies inputs to one or more mathematically independent nonlinear output functions for generation of multiple key-stream outputs per clock cycle
Patent Assignee: HUGHES AIRCRAFT CO (HUGA)
Inventor: BIANCO M E; MAYHEW G L
Number of Countries: 004 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 615361	A1	19940914	EP 94103796	A	19940311	H04L-009/18	199435 B
US 5365588	A	19941115	US 9330687	A	19930312	H04L-009/00	199445

Priority Applications (No Type Date): US 9330687 A 19930312
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
EP 615361	A1			

Designated States (Regional): DE FR GB
Language, Pages: EP 615361 (E, 11); US 5365588 (11)
...Abstract (Equivalent): of the working register into selected inputs of the intermediate stages, as determined by a **cryptographic** key. N mathematical **independent** nonlinear output function, where Ngreater than2, each for performing a different nonlinear function on the...

10/3,K/8 (Item 6 from file: 351)
DIALOG(R)File 351:DERWENT WPI

010004394 **Image available**
WPI Acc No: 94-272105/199433
Related WPI Acc No: 93-045088; 93-242755
XRPX Acc No: N94-214173
Algorithm independent cryptographic **key management appts. - selects one of several ciphering devices automatically using algorithm common to transmitting and receiving terminals**
Patent Assignee: MOTOROLA INC (MOTI)
Inventor: ALTSCHULER B N; HARDY D A; LEWIS L K
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5341427	A	19940823	US 91777870	A	19911016	H04L-009/08	199433 B
			US 92954205	A	19920930		
			US 9352438	A	19930423	B	

Priority Applications (No Type Date): US 91777870 A 19911016; US 92954205 A 19920930; US 9352438 A 19930423
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
US 5341427	A	Div ex	US 91777870	
		Div ex	US 92954205	
		Div ex		US 5179591
		Div ex		US 5230020

Language, Pages: US 5341427 (12)

Algorithm independent cryptographic **key management appts...**

10/3,K/9 (Item 7 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

009892284 **Image available**
WPI Acc No: 94-172200/199421
XRPX Acc No: N97-381358
Image processing apparatus for processing signals from scanner or camera etc - has second encrypting device capable of supplying encrypted image data to second apparatus different from first apparatus
Patent Assignee: CANON KK (CANO)
Inventor: ISHIMOTO K; KURITA M; SUZUKI Y
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
JP 6113154	A	19940422	JP 92258212	A	19920928	H04N-001/44	199421 B
US 5668881	A	19970916	US 93126649	A	19930927	G09C-005/00	199743 T

Priority Applications (No Type Date): JP 92258212 A 19920928
Language, Pages: JP 6113154 (19); US 5668881 (20)

...Abstract (Basic): to a second apparatus different from the first apparatus. The first and second encrypting devices **independently** execute the **encryption** . The first apparatus is an image memory device, and the second apparatus is a printer...

10/3,K/10 (Item 8 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

009549205 **Image available**
WPI Acc No: 93-242755/199330
Related WPI Acc No: 93-045088; 94-272105
XRPX Acc No: N93-186804
Algorithm independent cryptographic **key management device - has encrypted data transmitting and receiving devices coupled to ciphering devices selected by automatic controller**

Patent Assignee: MOTOROLA INC (MOTI)
Inventor: ALTSCHULER B N; HARDY D A; LEWIS L K
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5230020	A	19930720	US 91777870	A	19911016	H04L-009/02	199330 B
			US 92954205	A	19920930		

Priority Applications (No Type Date): US 91777870 A 19911016; US 92954205 A 19920930
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
US 5230020	A	Div ex	US 91777870	
		Div ex		US 5179591

Language, Pages: US 5230020 (10)

Algorithm independent cryptographic **key management device...**

10/3,K/11 (Item 9 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

009351614
WPI Acc No: 93-045088/199305
Related WPI Acc No: 93-242755; 94-272105
XRPX Acc No: N93-034587
Algorithm independent cryptographic **key management - exchanging first message for determining common key generation and ciphering method and comparing further shared messages**
Patent Assignee: MOTOROLA INC (MOTI)
Inventor: ALTSCHULER B N; HARDY D A; LEWIS L K
Number of Countries: 014 Number of Patents: 010
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5179591	A	19930112	US 91777870	A	19911016	H04L-009/02	199305 B
EP 537971	A2	19930421	EP 92309291	A	19921013	H04L-009/08	199316
AU 9222020	A	19930429	AU 9222020	A	19920901	H04L-009/12	199324
NO 9203371	A	19930419	NO 923371	A	19920828	H04L-000/00	199324
JP 5227152	A	19930903	JP 92290804	A	19921005	H04L-009/06	199340
AU 655304	B	19941215	AU 9222020	A	19920901	H04L-009/12	199506
EP 537971	A3	19940126	EP 92309291	A	19921013	H04L-009/02	199517
EP 537971	B1	19970212	EP 92309291	A	19921013	H04L-009/08	199712
DE 69217440	E	19970327	DE 617440	A	19921013	H04L-009/08	199718
			EP 92309291	A	19921013		
IE 80441	B	19980715	IE 922612	A	19920826	H04L-009/08	199835

Priority Applications (No Type Date): US 91777870 A 19911016
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
EP 537971	A2			
		Designated States (Regional): CH DE DK FR GB IT LI NL SE		
AU 655304	B	Previous Publ.		AU 9222020
EP 537971	B1			
		Designated States (Regional): CH DE DK FR GB IT LI NL SE		
DE 69217440	E	Based on		EP 537971

Language, Pages: US 5179591 (11); EP 537971 (E, 12); EP 537971 (E, 13)

Algorithm independent cryptographic **key management...**

10/3,K/12 (Item 10 from file: 351)
DIALOG(R)File 351:DERWENT WPI
(c)1998 Derwent Info Ltd. All rts. reserv.

009289939 **Image available**
WPI Acc No: 92-417348/199251

XRPX Acc No: N92-318264
Data processing system with cryptographic services facility - includes multiple client units and cryptographic services facility, with facility providing cryptographic services to client units
Patent Assignee: INT COMPUTERS LTD (INCM)
Inventor: PRESS J
Number of Countries: 008 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 518466	A1	19921216	EP 92303352	A	19920414	G06F-012/14	199251 B
AU 9218217	A	19921217	AU 9218217	A	19920612	G06F-012/14	199306
ZA 9203080	A	19930127	ZA 923080	A	19920428	G09C-000/00	199310
US 5253297	A	19931012	US 92874734	A	19920427	H04L-009/00	199342
AU 653823	B	19941013	AU 9218217	A	19920612	G06F-012/14	199442
EP 518466	B1	19980603	EP 92303352	A	19920414	G06F-012/14	199826
DE 69225745	E	19980709	DE 625745	A	19920414	G06F-012/14	199833
			EP 92303352	A	19920414		

Priority Applications (No Type Date): GB 9112644 A 19910612
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
EP 518466	A1			
		Designated States (Regional): BE DE FR GB IT		
AU 653823	B	Previous Publ.		AU 9218217
EP 518466	B1			
		Designated States (Regional): BE DE FR GB IT		
DE 69225745	E	Based on		EP 518466

Language, Pages: EP 518466 (E, 8); ZA 9203080 (20); US 5253297 (7); EP 518466 (E)

...Abstract (Basic): ADVANTAGE - Allow user to interface with **cryptographic** facility in algorithm-**independent** manner...

10/3,K/13 (Item 11 from file: 351)
DIALOG(R)File 351:DERWENT WPI

009122278 **Image available**
WPI Acc No: 92-249715/199230
XRPX Acc No: N92-190802
Multichannel data encryption device with parallel bus - has monitor processor connected to parallel bus with number of independently **operating data** encryption **boards within housing unit having tamper-detection mechanism**
Patent Assignee: EXCHANGE SYSTEM LP (EXCH-N)
Inventor: BASS T M; HAMILTON S B; ROSENOW M J
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5128996	A	19920707	US 88282415	A	19881209	H04L-009/00	199230 B

Priority Applications (No Type Date): US 88282415 A 19881209
Language, Pages: US 5128996 (302)

... **has monitor processor connected to parallel bus with number of** independently **operating data** encryption **boards within housing unit having tamper-detection mechanism**
...Abstract (Basic): the parallel bus and a serial port for connection to a host computer. Each data **encryption** board operates **independently** of the other data **encryption** boards...

10/3,K/14 (Item 12 from file: 351)
DIALOG(R)File 351:DERWENT WPI

009108409 **Image available**
WPI Acc No: 92-235839/199229
XRPX Acc No: N92-179577
Recording of signature for payment transactions - compares signature with encrypted signature to enable verification
Patent Assignee: NCR INT INC (NATC); AT & T GLOBAL INFORMATION SOLUTIONS INT INC (AMTT); NCR CORP (NATC)
Inventor: KAPP M A; ONEGA A M; PROTHEROE R L; ONEGA A
Number of Countries: 004 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
EP 494796	A2	19920715	EP 92300241	A	19920110	G07F-019/00	199229 B
US 5195133	A	19930316	US 91640199	A	19910111	H04L-009/32	199313
US 5297202	A	19940322	US 91640199	A	19910111	H04L-009/32	199411
			US 92979817	A	19921120		
EP 494796	A3	19960306	EP 92300241	A	19920110	G07F-019/00	199624
EP 494796	B1	19980415	EP 92300241	A	19920110	G07F-019/00	199819
DE 69225080	E	19980520	DE 625080	A	19920110	G07F-019/00	199826
			EP 92300241	A	19920110		

Priority Applications (No Type Date): US 91640199 A 19910111; US 92979817 A 19921120
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
EP 494796	A2			
		Designated States (Regional): DE FR GB		
US 5297202	A	Cont of	US 91640199	
		Cont of		US 5195133
EP 494796	B1			
		Designated States (Regional): DE FR GB		
DE 69225080	E	Based on		EP 494796

Language, Pages: EP 494796 (E, 19); US 5195133 (18); US 5297202 (18); EP 494796 (E, 21)

...Abstract (Equivalent): key which may be obtained from the transaction data. The encrypted record requires a second **decryption** key **independent** of the transaction data...

10/3,K/15 (Item 13 from file: 351)
DIALOG(R)File 351:DERWENT WPI

008961324 **Image available**
WPI Acc No: 92-088593/199211
XRPX Acc No: N92-066504
Communicating TV or digital audio signals in standard line - replacing analog video information in window transmitted during horizontal blanking interval with TDM digital audio signals
Patent Assignee: GEN INSTR CORP (GENN)
Inventor: KATZNELSON R D; M ; MORONEY P; SHUMATE W A
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5091936	A	19920225	US 91647827	A	19910130		199211 B

Priority Applications (No Type Date): US 91647827 A 19910130
Language, Pages: US 5091936 (13)

...Abstract (Basic): a video signal with an associated audio channel, or asa multiple channel digital audio signal. **Independent encryption** and **decryption** of each of the multiple audio channels is provided...

10/3,K/16 (Item 14 from file: 351)
DIALOG(R)File 351:DERWENT WPI

008837191 **Image available**
WPI Acc No: 91-341207/199147
XRPX Acc No: N91-261262
Coding appts. with fault display for data terminal - has control for receive and send channels with assigned crypto-generators and internal monitor
Patent Assignee: SIEMENS AG (SIEI)
Inventor: BETTENHAUS H; BETTENHAUSEN H
Number of Countries: 015 Number of Patents: 006
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 4023131	C	19911121	DE 4023131	A	19900720		199147 B
WO 9202086	A	19920206					199208
EP 540536	A1	19930512	EP 91912135	A	19910703	H04L-009/00	199319
			WO 91DE550	A	19910703		
US 5303293	A	19940412	WO 91DE550	A	19910703	H04K-001/00	199414
			US 92946488	A	19921103		
EP 540536	B1	19950329	EP 91912135	A	19910703	H04L-009/00	199517
			WO 91DE550	A	19910703		
DE 59105061 G		19950504	DE 505061	A	19910703	H04L-009/00	199523
			EP 91912135	A	19910703		
			WO 91DE550	A	19910703		

Priority Applications (No Type Date): DE 4023131 A 19900720
Filing Details:

Patent	Kind	Filing Notes	Application	Patent
WO 9202086	A			
		Designated States (National): US		
		Designated States (Regional): AT BE CH DE DK ES FR GB GR IT LU NL SE		
EP 540536	A1	Based on	WO 9202086	
		Designated States (Regional): CH DE GB IT LI NL		
US 5303293	A	Based on	WO 9202086	
EP 540536	B1	Based on	WO 9202086	
		Designated States (Regional): CH DE GB IT LI NL		
DE 59105061 G		Based on	EP 540536	
		Based on	WO 9202086	

Language, Pages: EP 540536 (G, 5); US 5303293 (5); EP 540536 (G, 8)

...Abstract (Equivalent): channels (S,E), an internal monitoring device (UA) assigned to the control device (C) for **independent** monitoring of the **cryptographic** device functions, and a display means (A) linked to the monitoring device (UA) for identification...
...Abstract (Equivalent): An internal monitoring device (UA) is assigned to the control device (C) for **independent** monitoring of the **cryptographic** device functions. A display (A) is linked to the monitoring device (UA) for identification of...

10/3,K/17 (Item 15 from file: 351)
DIALOG(R)File 351:DERWENT WPI

008659821 **Image available**
WPI Acc No: 91-163848/199122
XRPX Acc No: N91-125585
Microcomputer-based encryption system - coupling several data encryption devices with data bus and loading key into each device in predefined group through data bus
Patent Assignee: EXCHANGE SYSTEM LTD (EXCH-N)
Inventor: HAMILTON S B
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 5016277	A	19910514	US 88283444	A	19881209		199122 B

Priority Applications (No Type Date): US 88283444 A 19881209

...Abstract (Basic): Several encryption devices are contained in unit where each of the data **encryption** devices are adapted for **independent** operation. The data **encryption** devices are coupled with a data bus where encryption key information may be programmed in...

10/3,K/18 (Item 16 from file: 351)
DIALOG(R)File 351:DERWENT WPI

008276798 **Image available**
WPI Acc No: 90-163799/199021
XRPX Acc No: N90-127154
Connection of secure conference calls - using code translation, AGC, coding decoding, encryption, summing and decryption circuits as well as user interface
Patent Assignee: NORTHERN TELECOM LTD (NELE)
Inventor: STEER D G; STRAWCZYNS L
Number of Countries: 002 Number of Patents: 002
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
US 4920565	A	19900424	US 88220190	A	19880718		199021 B
CA 1292540	C	19911126					199203 N

Priority Applications (No Type Date): US 88220190 A 19880718

...Abstract (Basic): ADVANTAGE - Bridging unit does not need to know any **encryption** keys and can function **independently** of **encryption** process. (15pp Dwg.No.4/6)

10/3,K/19 (Item 17 from file: 351)
DIALOG(R)File 351:DERWENT WPI

007908745 **Image available**
WPI Acc No: 89-173857/198924
XRPX Acc No: N89-132719
Switch for linear fed-back shift register - has feedback terminal in each stage fitted in front of modulo-two adder
Patent Assignee: RADIOCOM AG (RADI-N)
Inventor: HARTMANN P
Number of Countries: 001 Number of Patents: 001
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Main IPC	Week
DE 3834741	A	19890608	DE 3834741	A	19881012		198924 B

Priority Applications (No Type Date): CH 874564 A 19871124
Language, Pages: DE 3834741 (6)

...Abstract (Basic): USE/ADVANTAGE - E.g. in data **encryption** . **Independent** mode of special application instance, but easy incorporation into wide range of circuits...
?

File 348:European Patents 1978-1998/Nov W48
(c) 1998 European Patent Office

Set	Items	Description
S1	15520	(INDEPENDENT? OR SEPARATE?)(N2) (LAYER? OR PROTOCOL?)
S2	10997	SECURITY? OR ENCRYPTION? OR DECRYPTION? OR CRYPTO?
S3	59	(SECURE()CHANNEL? OR JAVA(N2)STREAM? OR JAVA()SECURE()CHANNEL?)
S4	27072	(FIRST AND SECOND)(N2)(NODE? OR PROCESS?)
S5	2025	COMMUNICATION?(N)PROTOCOL?
S6	10	((COMMUNICATION?)(N2)(CHANNEL? OR PROTOCOL?))(N50)(S2(N3)INDEPENDENT?)
S7	0	S3 AND S1
S8	259	S1 AND S2
S9	20	S8 AND S5
S10	41	(INDEPENDENT?) (N4) (ENCRYPTION? OR CRYPTO? OR DECRYPTION? OR DECRYPTION?)
S11	2	S10 (S) ((COMMUNICATION?) (N2) (PROTOCOL? OR CHANNEL?))
S12	12	S1(N10)S2
S13	0	S12 NOT SEPARATE?
S14	0	S12(S)S5

9/3,K/1
DIALOG(R)File 348:European Patents

00936861
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
User terminal for mobile communications
Teilnehmer-Endgerat fur mobile Kommunikationen
Terminal d'abonne pour communications mobiles
PATENT ASSIGNEE:
NOKIA MOBILE PHONES LTD., (997961), P.O. Box 86, 24101 Salo, (FI),
(applicant designated states:
AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Korpela, Mikko, Autoilijantie 4B, 92130 Raahe, (FI)
LEGAL REPRESENTATIVE:
Frain, Timothy John et al (50188), Nokia Mobile Phones, St. George's Court, St. George's Road, 9 High Street, Camberley, Surrey GU15 3QZ, (GB)
PATENT (CC, No, Kind, Date): EP 852448 A1 980708 (Basic)
APPLICATION (CC, No, Date): EP 97300015 970102;
PRIORITY (CC, No, Date): EP 97300015 970102
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04Q-007/32;
ABSTRACT WORD COUNT: 105

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	9828	982
SPEC A	(English)	9828	4132
Total word count - document A			5114
Total word count - document B			0
Total word count - documents A + B			5114

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...SPECIFICATION or more common protocol radio access networks, and the backbone networks operate using technically incompatible **communications protocols** .
One way of implementing such systems would be to provide a full set of protocol...

...format (e.g. radio access format), and to utilise two or more different higher level **communication protocols** (corresponding to those utilised by different backbone networks), and further includes a control device for...

...is envisaged that networks may evolve over time, so that a mobile terminal with preset **communications protocols** would, at best, be unable to make full use of the available networks and, at...

...Accordingly, in preferred embodiments, the mobile terminal is arranged to be reprogrammable to use new **communications protocols** corresponding to new or amended backbone network **communications protocols** .
It would be possible to reprogram each mobile terminal by returning it to the factory...

...embodiment, we provide a mobile terminal which is arranged to download data relating to new **communications protocols** via the physical layer (e.g. radio access network).
In one preferred embodiment, the data...

...network components are arranged to perform signalling dialogue to automatically download data relating to new **communications protocols**

when the transmitted signal indicating the backbone networks to which the radio access network is...

...Figure 5;

Figure 7 corresponds to Figure 6 and illustrates the functional components of the **communications protocol** software present in the radio access network of Figure 3;

Figure 8 illustrates the structure...

...into packets, ATM cells or a TDM bit stream and into a frame structure); data **encryption** ; redundancy reduction encoding and decoding; and other functions which are of themselves known.

The RF...component, a B-ISDN MM component; and a B-ISDN adaptation component, and a packet **communications protocol** file 153 comprises an internet protocol (IP) component; an SNDCP-U packet radio component; and a adaptation component.

Each component of each protocol file therefore corresponds to a **separate layer protocol** , and communicates with the layers above and below by the exchange of so-called "primitives...

...CLAIMS wireless communication interface (21, 22) for communicating with a mobile terminal (10) employing low level **communications protocols** , and a plurality of network protocol interfaces (23a, 23b) for coupling to respective different communications networks (30, 30b) employing respective different, incompatible, relatively high level **communications protocols** .

16. Apparatus according to claim 15 further comprising means (25) for periodically transmitting a signal...

...to claim 17, in which each said record (261-263) comprises a representation of said **protocols** which is **independent** of the construction of a said terminal (10).

19. Apparatus according to claim 18 in...

9/3,K/2

DIALOG(R)File 348:European Patents

00919753
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

Multifunction occupancy sensor
Anwesenheitssensor mit mehreren Funkionen
Capteur de presence multifonctionnel

PATENT ASSIGNEE:
HUBBELL INCORPORATED, (775242), 584 Derby Milford Road, Orange, Connecticut 06477, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FI;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Baldwin, John R., 8 Botsford Lane, Newtown, Connecticut 06470, (US)
Batko, Thomas J., 159 Coook Hill Road, Wallingford, Connecticut 06492, (US)
Ellison, David F., 9 Sherwood Drive, Westport, Connecticut 06880, (US)
LEGAL REPRESENTATIVE:
Dixon, Donald Cossar et al (30122), Gee & Co. Chancery House Chancery Lane, London WC2A 1QU, (GB)

PATENT (CC, No, Kind, Date): EP 838792 A2 980429 (Basic)
APPLICATION (CC, No, Date): EP 97308048 971010;
PRIORITY (CC, No, Date): US 738045 961025
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: G08B-013/19;
ABSTRACT WORD COUNT: 265

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count
CLAIMS A (English) 9818 1036

SPEC A (English) 9818 4745
Total word count - document A 5781
Total word count - document B 0
Total word count - documents A + B 5781

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...ABSTRACT A2
A multifunction passive infrared occupancy sensor (14) which functions as an occupancy sensor for **security** systems and also as an occupancy sensor for energy management control systems. The occupancy sensor...

...representative thereof. A processing means (97) analyzes the output signal of the detector (91) for **security** detection purposes by detecting changes in the output signal greater than a given **security** threshold. The processing means (97) also analyzes the output signal of the detector (91) for...

...the output signal greater than a given energy management threshold, which is less than the **security** threshold. In one embodiment (Fig. 5) first and second processing circuits detect changes in the detector output signal greater than the **security** threshold and energy management threshold. In a second embodiment (Fig. 6) the output of the...

...to a digital processor (68) which utilizes one of two different software processing routines, a **security** threshold processing routine, and an energy management threshold processing routine. A further embodiment (Fig. 9...

...SPECIFICATION invention relates to a multifunction occupancy sensor which provides a first occupancy output signal for **security** systems and a second occupancy output signal for energy management control systems. The multifunction occupancy...

...the occupied space networked environment. The multifunction network sensor system further comprises energy management and **security** controller systems, and a common data communication network which connects to the multifunction sensor and...

...systems, Demand Side Management (DSM) electrical load management control systems, presence monitoring systems, and for **security** sensing in **security** systems, although modules combining occupancy sensing and ambient light sensing have been used in nonnetworked systems.
In general, the tripping of an occupancy sensor in a **security** system has more serious consequences than the tripping of an occupancy sensor in an energy...

...a controlled lighting environment. In contrast thereto, the tripping of an occupancy sensor in a **security** system can result in the dispatching of **security** personnel or police to the monitored premises to personally check the premises for a **security** breach or intrusion. If the alarm turns out to be a false alarm, a substantial...

...wavelength, are well known in the art, and are frequently used as occupancy sensors in **security** systems, and in energy management control systems such as lighting control systems or HVAC systems...

...view of the detector. Accordingly, such PIR sensors can be used as occupancy sensors in **security** systems and also in energy management control systems such as in lighting control systems or...

...DSM systems and also in presence monitoring systems.
In order to make occupancy sensors in **security** systems more reliable and accurate, as compared to occupancy sensors in energy management systems, occupancy sensors for **security** systems are characterized by basic design differences, among which are the following key differences: (1...

security threshold.
6. A multifunction passive infrared occupancy sensor as claimed in any of claims 1...

...as an energy management control sensor with a greater circuit amplification gain or as a **security** sensor with a less circuit amplification gain.
7. A multifunction passive infrared occupancy sensor as...
...sensor by adding sensing elements, and to increase the field of view intensity for the **security** sensor by subtracting sensing elements.
8. A multifunction passive infrared occupancy sensor as claimed in...

...in claim 1, wherein the lens means comprises a first optical lens array designed for **security** and having a first number of lens segments, and a second optical lens array designed...

...as claimed in claim 1 or claim 10, wherein the detection means comprises a separate **security** detector and a separate energy management detector, and further comprises a separate **security** amplifier having a **security** amplification gain, and a separate energy management amplifier having an energy management circuit amplification gain which is greater than the **security** amplification gain.
12. A multifunction passive infrared occupancy sensor as claimed in claim 11, wherein the ratio of energy management amplifier gain to the **security** amplifier gain is in the range of 3:1 to 5:1.
13. A multifunction...energy management control sensor and when a detected event occurs, the sensor switches to a **security** sensor configuration for a period of time and looks for **security** detected, events are detected, and if no **security** events are detected, the sensor returns to an energy management control sensor.

9/3,K/3
DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00782450
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Configurable hybrid medium access control for cable metropolitan area networks
Zugangskontrolle fur ein konfigurierbares Hybridmedium in metropolitanen Kabelnetzwerken
Controle d'acces pour support hybride configurable pour reseaux metropolitains cables
PATENT ASSIGNEE:
GENERAL INSTRUMENT CORPORATION, (264772), 2200 Byberry Road, Hatboro, Pennsylvania 19040, (US), (applicant designated states: BE;DK;GB;NL;SE)
INVENTOR:
Safadi, Reem, 429 Brown Briar Circle, Horsham, PA 19044, (US)
LEGAL REPRESENTATIVE:
Boydell, John Christopher (28571), Stevens, Hewlett & Perkins 1 Serjeants' Inn Fleet Street, London EC4Y 1LL, (GB)
PATENT (CC, No, Kind, Date): EP 730382 A2 960904 (Basic)
EP 730382 A3 970423
APPLICATION (CC, No, Date): EP 96301369 960228;
PRIORITY (CC, No, Date): US 395325 950228; US 402007 950310
DESIGNATED STATES: BE; DK; GB; NL; SE
INTERNATIONAL PATENT CLASS: H04N-007/173;
ABSTRACT WORD COUNT: 198

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	1021
SPEC A	(English)	EPAB96	9345
Total word count - document A			10366

Total word count - document B 0
Total word count - documents A + B 10366

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...SPECIFICATION related to co-pending application Serial No. 08/402,027 filed concurrently herewith, entitled ADAPTIVE **PROTOCOL COMMUNICATION** SYSTEM to Reem Safadi which is incorporated by reference as if fully set forth herein...located), an operations support system (OSS) 28 (co-located or remotely located), an integrated transport **encryption** multiplexer (ITEM) 30, a 64 quadrature amplitude modulation (QAM) modulator 32, an RF upconverter 34...12/L2G). The ASEM 22 forwards appropriate scheduling parameters to the addressable controller 24 for **encryption** of pay-per-view (PPV) and impulse-pay-per-view (IPPV) services by the ITEMs...

...demand (staggercast) services, including VIU authorization for those services and program scheduling by controlling the **encryption** subsystem. Access control and **encryption** parameters are forwarded to network elements which perform downstream and upstream **encryption** and **decryption** . In the preferred embodiment of the invention, downstream **encryption** is implemented in the ITEMs 30, 50 and downstream **decryption** is implemented in network modules 70, which are part of each STT 16. Upstream **encryption** is implemented in the network module 70 and upstream **decryption** is performed by a network controller 62. For interactive service communications, which are facilitated at...

...addressable controller 24 preprovisions the ITEMs 50 and the network modules 70 with the appropriate **encryption /decryption** parameters. For broadcast service communications, which are facilitated by the hub 14, the addressable controller...

...on scheduling information forwarded by the L1G 20 through the ASEM 22.

The integrated transport **encryption** multiplexer (ITEM) 30 provides secure delivery of broadcast digital services information to the VIUs as ...

...maintained end-to-end. The resulting MPEG2 transport multiplex (consisting of multiple audiovisual information streams, **protocol - independent** , from an ITEM 30 standpoint, information streams carried as AAL5-SDUs (such as stock quotes...

...a given set of MPEG2 program streams within the MPEG2 transport stream. Access control and **encryption** related information is forwarded to ITEM 30 from the addressable controller 24. The ITEM 30...The network module 70 also communicates with the addressable controller 24 for access control and **decryption /encryption** authorization.

The QPSK demod/mux 60 receives up to six upstream carriers, demodulates the carriers...selected channel if the VIU is an authorized user. Similarly, digital video passes through the **decryption** and then MPEG2 decodes and D/A conversion to forward the composite video for display...

...tuner 110 and descrambler 112 are controlled by the network module 70, which includes an **encryption /decryption** controller 124 and a MAC module 126.

The network module 70 interfaces with a processor...400 is shown. The STT 16 includes a medium access control module 126 and a **decryption / encryption** control module 124 for communicating with the network controller 62 through the transmission network 56...

9/3,K/4
DIALOG(R)File 348:European Patents

00726329
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Improved channel interfaces for computer input/output channels.
Verbesserte Kanalschnittstellen fur Rechnerein-/ausgabekanale.
Interfaces de canal ameliorees pour canaux d'entree-sortie d'ordinateur.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Barrett, Linda, 6001 Wintergreen Drive, Raleigh, NC 27609, (US)
Stagg, Arthur James, 12613 Waterman Drive, Raleigh, NC 12714, (US)
Long, Lynn Douglas, 2911 Meacham Road, Chapel Hill, NC 27516, (US)
Ward, Raymond Edward, 812 Bluestone Road, Durham, NC 27713, (US)
Menditto, Louis Frank, 4701 Tanglewood Drive, Raleigh, NC 27612, (US)
LEGAL REPRESENTATIVE:
de Pena, Alain (15151), Compagnie IBM France Departement de Propriete Intellectuelle, 06610 La Gaude, (FR)
PATENT (CC, No, Kind, Date): EP 685952 A1 951206 (Basic)
APPLICATION (CC, No, Date): EP 95480055 950427;
PRIORITY (CC, No, Date): US 252020 940601
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-029/06; G06F-013/38;
ABSTRACT WORD COUNT: 108

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	723
SPEC A	(English)	EPAB95	8347
Total word count - document A			9070
Total word count - document B			0
Total word count - documents A + B			9070

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...ABSTRACT to define and activate unbalanced groups of unidirectional communications sub-channels for a user application. **Protocol independent** exchange identifications permit not only unbalanced transmission groups but also allow user-controlled extensions for...

...SPECIFICATION unique sub-channels during their installation and communication over that sub-channel conformed to the **communication protocols** defined for that type of I/O device. Note that all sub-channels in the...the necessary parameters between the two ends of the sub-channel. Some form of system **security** is also desirable to ensure that the two ends of the sub-channels have the...

...diversified channel environment gives rise to a number of system design problems.
For example, channel **security** was easy to ensure when distances were limited to units expressed in terms of meters...

...expands that distance to world-wide connectivity. In addition, earlier systems provided a degree of **security** by the use of pre-defined, static definitions. The flexibility of dynamic definitions also gives...which include the negotiation of system parameters and the provision of user-supplied system verification (**security**) fields (e.g., encrypted passwords). The exchange of system parameters such as buffering size and ...

...the user data with the appropriate protocol processing and makes the sub-channel control process **independent** of the **protocol** of the user application 10 of FIG. 1. PDU header 26 also includes a sequence... protocols makes the entire operation of the multi-path channel interface of the present invention **independent** of the **protocol** of the user application. This protocol independence permits a very wide variety of users to...

...MPC. Both the local and the remote MPC interfaces also verify system integrity and system **security** fields in the received XID-1 messages. Finally, differences in requests for data handling parameters...noted above, the protocol identification fields, such as field 93 in FIG. 5, can include **security** information such as system identifications which are checked to determine whether or not communication is...

...CLAIMS comprising at least one user application operating in said computer system according to a predetermined **communications protocol** to communicate blocks of data to a remote data utilization system over a communications channel...

...2, 3 or 4 further comprising means in said message for selectively identifying said predetermined **communications protocol** .
6. The input and output communications subsystem according to anyone of claims 1 to 5 further comprising means in said message for testing the **security** of said sub-channel.
7. A method for input and output communications in a general...

...comprising executing at least one user application in said computer system according to a predetermined **communications protocol** to communicate blocks of data to a remote data utilization system over a communications channel...

...anyone of claims 7 to 10 further comprising the step of selectively identifying said predetermined **communications protocol** in a portion of said message.
12. The method according to anyone of claims 7...
...comprising the step of utilizing one or more fields of said message for testing the **security** of said sub-channel. ...

9/3,K/5
DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00720054
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Open transaction manager access system and method.
Offenes Transaktionverwaltungszugriffsystem und Verfahren.
Systeme et methode ouvert de gestion des transactions d'acces.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Lai, Robert Shiwen, 1131 Valley Quail Circle, San Jose, California 95120, (US)
Millar, Robert Daniel, 7 Glenesha Gardens, Fareham, Hampshire PO15 6QH, (GB)
Radke, Harry Otto, 16 Cheltenham Way, San Jose, California 95139, (US)
LEGAL REPRESENTATIVE:
Moss, Robert Douglas (34141), IBM United Kingdom Limited Intellectual Property Department Hursley Park, Winchester Hampshire SO21 2JN, (GB)
PATENT (CC, No, Kind, Date): EP 681387 A2 951108 (Basic)
APPLICATION (CC, No, Date): EP 95301775 950316;
PRIORITY (CC, No, Date): US 210977 940321
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-029/06;
ABSTRACT WORD COUNT: 91

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	899
SPEC A	(English)	EPAB95	6277
Total word count - document A			7176

Total word count - document B 0
Total word count - documents A + B 7176

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...SPECIFICATION The log-in procedure establishes the attributes of message handling, also referred to as the **communication protocol** , that will be followed by the host computer for the receiving of transactions from the...

...word size and error detection and correction.
Generally, a user is bound to the established **communication protocol** for the duration of the session. Session binding of the **communication protocol** takes place via control blocks that are created at the beginning of each session. The...

...protocol, and therefore the host computer and information management system must accommodate a variety of **communication protocols** . Moreover, the networks in which the terminals might be connected could have different protocols. Again, the host computer system must support whatever **communication protocol** is being used by the attached network to receive messages from users, perform the necessary...

...the information management system uses internally, and then convert the transaction response back into the **communication protocol** of the user for return.
Fig. 1, for example, shows a computer processing system 10...

...The connection processor establishes a communication session with each user terminal such that the terminal **communication protocol** will be recognized and transaction output will be properly directed. Each session is associated with...

...that receive transactions from one of the user terminals through the connection processor, recognize the **communication protocol** being used by the terminal, and process the ...of the communication session.
The user terminals 14 can potentially use any one of many **communication protocols** . For example, the terminals may communicate using an IBM Corporation protocol known as a "SNA...

...and RPC. A different protocol interface module ("DDM") must be provided for each type of **communication protocol** that will be supported by the host computer 12. For each supported protocol, the connection...

...the half duplex "DDM" modules frequently must communicate with full duplex user terminals and complex **communication protocols** , the "DDM" modules can be quite complicated and difficult to create.
As can be seen...

...DDM" modules, that can directly bridge the protocol gap between older system architectures and newer **communication protocols** . Moreover, some of the newer protocols are capable of performance that cannot be supported by...

...a transaction protocol, for each one of a plurality of transactions, independently of any predefined **communications protocol** , based on said attributes;
means for dynamically binding said transaction protocol to said one transaction...

...on said attributes, for each one of a plurality of transactions independently of a predefined **communication protocol** , a transaction protocol comprising a synchronization paradigm and a flow control, said transaction protocol then...The system treats transactions as objects to facilitate a separate transaction-specific, application and session **independent layer** in a communications architectural model. Thus, users are provided with greater flexibility in their transaction...

...the transaction processing system illustrated in Fig. 2.
Fig. 9 is a representation of the **security** data of the transaction protocol used by the transaction processing system illustrated in Fig. 2 ...

...transaction manager 124. The user terminals send their transactions to the adapter appropriate for the **communication protocol** they are using. For each transaction that is received, the adapters recognize the **communication protocol** being used by the terminal and provide a transaction protocol that can be understood by...join.
At the next diagram block 204, the adapter receives the transaction and recognizes the **communication protocol** of the user terminal. Next, at the next diagram block 206, the adapter isolates the...which prefixes are attached to the message. The prefixes can comprise, for example, state data, **security** data, user data, or application data, or any combination thereof.
The next data field illustrated...

...field is for a token representing the message destination.
Fig. 9 is a representation of **security** data information and illustrates novel **security** features provided by the transaction processing system constructed in accordance with the present invention. The first **security** data field is the length of the information, including the length field itself. The next data field is for a **security** flag, which can be set to indicate to the information management system that the user terminal has already gone through **security** verification procedures at the adapter level and which do not have to be repeated. In general, transaction protocols require **security** to be verified immediately before access to the information management system is granted. In accordance with the present invention, then, the adapters can perform **security** verification duties and therefore can eliminate duplicative **security** processing with the **security** flag data field. This can greatly reduce the amount of processing overhead.
The next three...

...the user identification itself, then the password length, the password type, the password itself, the **security** profile length not including the length field itself, the profile type, and the profile itself... considerations. As such, the invention can be implemented as a unique, transaction-specific reference model **layer** that is **independent** of the other layers. Thus, the protocol described above is not specific to any application...

...CLAIMS a transaction protocol, for each one of a plurality of transactions, independently of any predefined **communications protocol** , based on said attributes;
means for dynamically binding said transaction protocol to said one transaction...

...process means for receiving the transactions from the transport means and determining said specified transaction **protocol independently** for each received transaction, each transaction protocol including a plurality of protocol data fields specifying...

...on said attributes, for each one of a plurality of transactions independently of a predefined **communication protocol** , a transaction protocol comprising a synchronization paradigm and a flow control, said transaction protocol then...

...claim 13 or claim 14, wherein the step of specifying further includes determining whether a **security** verification step has been performed and is not to be repeated.
16. A method as...

9/3,K/6

DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00693309
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Automated benchmarking with self customization.
Automatische Messung der Zeit der Arbeitung mit Selbstbenutzeranpassung.
Mesure automate de vitesse de traitement avec autopersonnalisation.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Daugherty, Raymond F., 5406 Ridge Road, Mt. Airy, MD 21771, (US)
Hershey, Paul C., 7612 Michelle Court, Manassas, VA 22110, (US)
Waclawsky, John G., 6105 Spring Meadow Lane, Frederick, MD 21701-5819, (US)
LEGAL REPRESENTATIVE:
Schafer, Wolfgang, Dipl.-Ing. (62021), IBM Deutschland Informationssysteme GmbH Patentwesen und Urheberrecht, D-70548 Stuttgart, (DE)
PATENT (CC, No, Kind, Date): EP 661847 A2 950705 (Basic)
APPLICATION (CC, No, Date): EP 94119305 941207;
PRIORITY (CC, No, Date): US 173530 931223
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-012/26;
ABSTRACT WORD COUNT: 236

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	1373
SPEC A	(English)	EPAB95	12156
Total word count - document A			13529
Total word count - document B			0
Total word count - documents A + B			13529

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...SPECIFICATION monitoring and controlling system to assess and to modify protocol activity for a variety of **communications protocols** . The protocols handled include Token Ring protocol, ETHERNET protocol, Fiber Distributed Data Interface (FDDI) protocol...

...of the expert system and Programmable Performance Vector Generator combination is also applied, to additional **communications protocols** such as Ethernet protocol, FDDI protocol, SNA protocols, TCP/IP protocols or the SONET protocol...

...significantly improve the functions, and services and management of any data communications network. It is **independent** of **communications protocols** , standards, and physical media. The Information Collection Architecture invention is physically connected to an existing...or will exceed in the future) some criteria that indicates a performance problem, or a **security** violation, or a billing error, etc.
The criteria that are used to evaluate whether the...

9/3,K/7
DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00603240
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Communications protocol **for exchanging interface information between a host and a terminal.**
Kommunikationsprotokoll zum Schnittstelleninformationsaustausch zwischen Host und Rechnerterminal.

Protocole de communication pour echange d'information d'interface entre un ordinateur central et un terminal.

PATENT ASSIGNEE:
AT&T Corp., (589373), 32 Avenue of the Americas, New York, NY 10013-2412, (US), (applicant designated states: GB;IT)
INVENTOR:
Ackerman, Chaim M., 752 S. Lake Drive, Lakewood, New Jersey 08701, (US)
Glasser, Alan L., 4 Sheffield Drive, Manalapan, New Jersey 07726, (US)
Klein, Rueben, 8 Mount Court, East Brunswick, New Jersey 08816, (US)
LEGAL REPRESENTATIVE:
Buckley, Christopher Simon Thirsk et al (28912), AT&T (UK) LTD., AT&T Intellectual Property Division, 5 Mornington Road, Woodford Green, Essex IG8 0TU, (GB)
PATENT (CC, No, Kind, Date): EP 606718 A2 940720 (Basic)
EP 606718 A3 981021
APPLICATION (CC, No, Date): EP 93309756 931206;
PRIORITY (CC, No, Date): US 998217 921230
DESIGNATED STATES: GB; IT
INTERNATIONAL PATENT CLASS: G06F-003/033;
ABSTRACT WORD COUNT: 126

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	3696
SPEC A	(English)	EPABF2	9288
Total word count - document A			12984
Total word count - document B			0
Total word count - documents A + B			12984

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

Communications protocol **for exchanging interface information between a host and a terminal.**

...ABSTRACT A2

The invention is directed to a **communications protocol** which facilitates the exchange of interface information between a host processor (200) and a terminal...

...SPECIFICATION A2

Field of the Invention

The invention relates to **communications protocols** and more particularly relates to a protocol for exchanging messages between a transaction processor and...

...Invention

Based on the foregoing, we have recognized that there is a need for a **communications protocol** that is **independent** of the host transaction processor as well as the operating characteristics of different types of ...

...host might communicate with. Thus, an advancement in the art is achieved by providing a **communications protocol** for exchanging application interface information between a host computer and user terminal, workstation or smart in the inventive **communications protocol** ;

FIG. 8 is an example of the way in which a particular pattern of objects...

...station set 10, and processor 200 communicate with one another in accord with the inventive **communications protocol** .

More particularly, processor 200 is a multiuser computer that is programmed to implement the principles...is used for storing information and data, such as, for example, credit card numbers, social **security** numbers, addresses, etc., that is personal to the user and, therefore, is not displayed on...discards the received message.

FIG. 12 illustrates in flow chart form the actions that the **communications protocol** program invokes with respect to receipt of a

particular type of command received from an...

...respectively.
FIGs. 13-15 show in flow chart form the program which implements the inventive **communications protocol** in a data terminal, such as a smart phone, e.g., station set 10 (FIG...

...CLAIMS discards the received message.
FIG. 12 illustrates in flow chart form the actions that the **communications protocol** program invokes with respect to receipt of a particular type of command received from an...

...respectively.
FIGs. 13-15 show in flow chart form the program which implements the inventive **communications protocol** in a data terminal, such as a smart phone, e.g., station set 10 (FIG...

9/3,K/8
DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00594069
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Cooperative processing interface and communication broker for heterogeneous computing environments
Zusammenarbeitende Rechnerschnittstelle und Kommunikationsmakler fur heterogene Umgebung
Interface de traitement cooperatif et courtier de communication pour environnement heterogene
PATENT ASSIGNEE:
SOFTWARE AG, (1710380), , Darmstadt, (DE), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IE;IT;LI;LU;MC;NL;PT;SE)
INVENTOR:
Page, Peter, Brueder-Knauss Strasse 39, D-64285 Darmstadt, (DE)
Warns, Ruediger, IM Wiesengrund 4, D-64665 Alsbach 2, (DE)
Graham Kennedy, Terence, Korellweg 16, D-64297 Darmstadt, (DE)
Ejtemai-Jandahi, Omid, Troyesstrasse 50, D-64297 Darmstadt, (DE)
LEGAL REPRESENTATIVE:
Kirschner, Klaus Dieter, Dipl.-Phys. (6506), Patentanwalt, Sollner Strasse 38, 81479 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 600235 A1 940608 (Basic)
EP 600235 B1 980218
APPLICATION (CC, No, Date): EP 93117599 931029;
PRIORITY (CC, No, Date): US 969722 921030
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE
INTERNATIONAL PATENT CLASS: H04L-029/06;
ABSTRACT WORD COUNT: 121

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9808	1518
CLAIMS B	(German)	9808	1534
CLAIMS B	(French)	9808	1894
SPEC B	(English)	9808	16444
Total word count - document A			0
Total word count - document B			21390
Total word count - documents A + B			21390

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...ABSTRACT operating systems and may be connected to computer networks having different network architectures and associated **communications protocols** . The broker manages the service offerings from servers and service requests from clients, and clients...

...SPECIFICATION platform, use the same operating system, and are interconnected using a single network architecture and **communication protocol** , connection and communication between applications and/or machines is straightforward. However, this ideal is seldom...

...s System Network Architecture ("SNA") and IBM's Logical Unit 6.2 ("LU 6.2") **communications protocol** , while LAN 7 might be based on a different architecture, such as OSI and its associated **communications protocol** . The **communications protocol** is a defined set of procedural rules which computers use to communicate across a network.

The use of different hardware platforms, operating systems, or network architectures and their associated **communications protocols** inhibits the useful exchange of information between clients and servers in a heterogeneous environment, such...calls. Such a system should support communication between applications independent of operating system, hardware, network/**communication protocol** , and programming language.

Summary of the Invention

The drawbacks of the prior art are overcome...

...operating systems and may be connected to computer networks having different network architectures and associated **communications protocols** . The broker manages the service offerings from servers and service requests from clients, and clients...

...service broker.

An adapter may also be provided as a gateway to convert a foreign **communications protocol** to the function server protocol to allow applications programs to access the service broker functionality...

...Each of the four LANs are based on a different network architecture, utilizing a different **communications protocol** , while each of clients 10 and servers 12 run different operating systems.

Service broker 14...s).

Service broker 14 also provides a number of services 20, such as directory services, **security** services, and accounting services.

II. COMMUNICATION WITH THE SERVICE BROKER

A. Client/Server Processing Types...

...content of the communication is carried by signals that are arranged according to a physical **communication protocol** 40 (such as SNA (LU 6.2), TCP/IP, DECnet, and LANs). To provide communication between participants and the service broker 14 that is independent of the physical **communications protocol** 40, one or more higher communication layers are required.

Accordingly, the communications network 22 provides...in the appropriate protocol format to the physical network.

The FSP is thus the common **communication protocol** to which the service broker and each participant must adhere at the LAPI 44. The...

...ID field identifies the user and is required, for example, if the broker is providing **security** services.

The Password field is used to prevent unauthorized access to a service as part of the **Security** Services.

With the Wait field, the caller can choose between synchronous and asynchronous processing by...broker will reconnect the user with the previous environment. This is subject to validation if **security** is in effect. This is not needed by applications that mask the location from the broker or in circumstances when the broker can uniquely identify the reconnection.

The **Security** Token field is only valid for certain types of **security** systems and is only then required if **security** is in effect. It provides a convenient means of user authentication and is returned to...

...a client/server only -- when a client/server has timed-out or

Deregistered, a new **security** token must be obtained.

The Send(underscore)Length field is necessary for SEND processing -- it ...as by translating data between ASCII and EBCDIC formats and performing data compression/decompression and **encryption /decryption** .

III. THE SERVICE BROKER'S STRUCTURE

The core or kernel of the broker consists of...of DEREGISTER. If associated with an individual Application it applies to the specific Application only.

SECURITY -- The broker uses this Attribute to invoke the required **Security** checks. The value STD invokes the standard routine that is supplied with the BROKER. If...it uses previously-used settings. The administrator can dynamically alter important application settings (such as **security**) by using the administrator functions.

The attributes can be placed on a variety of storage...proper authority, which is defined in the directory by the administrator and is verified (if **security** has been activated).

To register one or more services with the broker, a participant passes ...Software A.G.'s REVIEW and IBM's SMF, or a straightforward serial file.

3. **Security**

The broker provides access to standard packages according to the platform to enable the administrator...prior to offering services to clients. Upon receipt of the register function, the broker performs **security** checks to determine if this server is allowed to register, and then makes a procedure...

...CLAIMS so, to communicate the service request to the server, the system being characterised by a **protocol independent** communications transport **layer** , said transport layer having a low level application programming interface LAPI and being adapted to...broker to the server, characterised by disposing between the participants and the physical network a **protocol independent** communications transport **layer** having a lower level application interface LAPI accepting messages from the participants via the LAPI...

9/3,K/9

00592044

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

An ally mechanism for inter-connecting distributed computing environment (DCE) and non-DCE systems to operate in a network system.

Partner-Mechanismus zum Verbinden von Systemen mit einer Umgebung fur verteilte Berechnungen (UVB) und non-UVB Systemen zum Betrieb in einem Netzwerksystem.

Mecanisme d'alliance pour interconnecter des systemes a environnement de calcul distribue (ECD) et des systemes non-ECD pour les faire operer dans un systeme re

PATENT ASSIGNEE:
Bull HN Information Systems Inc., (405375), Corporation Trust Center 1209 Orange Street, Wilmington Delaware, (US), (applicant designated states: DE;ES;FR;GB;IT)

INVENTOR:
Stein, Scott A., 10433 N. 9th Street, Phoenix, AZ 85020-1584, (US)
Carlson, Bruce M., 2922 W. Hartford Drive, Phoenix, AZ 85023, (US)
Yen, Chung S., 5 Karen Drive, Bedford, MA 01730, (US)
Farrington, Kevin M., 131 Canterbury Square, Williamsville, NY 14221, (US)

LEGAL REPRESENTATIVE:
Altenburg, Udo, Dipl.-Phys. et al (1266), Patent- und Rechtsanwalte Bardehle . Pagenberg . Dost . Altenburg . Frohwitter . Geissler & Partner Postfach 86 06 20, D-81633 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 590519 A2 940406 (Basic)
EP 590519 A3 940518

APPLICATION (CC, No, Date): EP 93115348 930923;
PRIORITY (CC, No, Date): US 951069 920925
DESIGNATED STATES: DE; ES; FR; GB; IT
INTERNATIONAL PATENT CLASS: G06F-009/46; G06F-015/16;
ABSTRACT WORD COUNT: 166

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	1049
SPEC A	(English)	EPABF2	11494
Total word count - document A			12543
Total word count - document B			0
Total word count - documents A + B			12543

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...ABSTRACT computer system which are loosely coupled together through a communications network operating with a standard **communications protocol** . The non-DCE and DCE computer systems operate under the control of proprietary and UNIX...

...SPECIFICATION with such systems in terms of the lack of distributed software, network communications and message **security** .
In general, the approach has been to port a substantial number of software services from...remote procedure call (RPC) service component including presentation service, a Naming (Directory) service component, a **Security** service component, a Threads service component, a Time service component and a Distributed file system...

...is based on the Apollo Network Computing System (NCS) which provides a clearly specified RPC **protocol** that is **independent** of the underlying transport layer and runs over either connectionless or connection oriented lower layers...

...service application programming interface (API) and the X/Open Directory Service (XDS) API.
The DCE **Security** Service component provides secure communications and controlled access to resources in the distributed system. There are three aspects to DCE **security** : authentication, secure communication, and authorization. These aspects are implemented by several services and facilities that together comprise the DCE **Security** Service, including the Registry Service, the Authentication Service, and Privilege Service, the Access Control List...

...by the Authentication Service. Communication is protected by the integration of DCE RPC with the **Security** Service-communication over the network can be checked for tampering or encrypted for privacy. Finally ...

...specified in the resource's Access Control List. The Login Facility initializes a user's **security** environment, and the Registry Service manages the information (such as user accounts) in the DCE **Security** database.
The DCE Threads Service component supports the creation, management, and synchronization of multiple threads...component, a call service component, a network listener service component, a binding service component, a **security** service component, an interface service component, an object service component, a communications management service component...

...call handle which is part of every function in the call service component.
The RPC **security** service component provides for the selection of four levels of **security** . These are the performance of authentication on every association establishment, the performance of authentication on... servers normally perform local services for client application program such as naming or directory services, **security** services and, time

with a **security** level set, the ally component 12-10 creates a proxy binding handle to the **security** service. This is returned to the client application as the imported binding. Meanwhile, the ally component 12-10 places the actual binding, as well as the **security** information, into its database for the forwarding service subcomponent 12-104 to use.
Whenever a...

...subcomponent 12-104 checks the database to determine whether the proxy binding has an associated **security** level. If so, the forwarding service subcomponent 12-104 passes the packet to the **security** service to have the relevant parts of the message encrypted according to the **security** information on the binding handle. The new packet is returned to the forwarding service subcomponent...

...the server. Similarly, packets transferred from the server to the client are passed through the **security** service subcomponent 12-103 to decrypt any data for the client system.
The above requires...

...that the ally system must track. For example, the client context contains all proxy bindings, **security** information, forwarding information, etc. The ally system returns a context handle to the client system...set of binding handles from the ally system. In a similar fashion, the DCE RPC **security** routines (e.g. sec...handle in the client database and checks to see if the client has requested a **security** level for this interface specification (e.g., printer interface). Also, the routine registers the **security** level information with the context handle and returns the CDS lookup context handle to the...call returns a vector of binding handles just as normal case if there is no **security** involved. Otherwise, the ally caches the vector of binding handles and returns a proxy binding...

...to try until it either succeeds or the list exhausts.
Without the involvement of the **security** , the proxy binding handle is not created until the list of binding handles was first...the other ally requests APIs are in a similar manner. For example, several of the **security** APIs form part of standard **security** DCE APIs (e.g. sec...

...CLAIMS to said request section, a naming service section coupled to said request section, and a **security** service section coupled to said request section.
8. The system of claim 1 wherein said...

9/3,K/10
DIALOG(R)File 348:European Patents

00555558
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
APPARATUS AND METHOD FOR CREATION OF A USER DEFINABLE VIDEO DISPLAYED DOCUMENT SHOWING CHANGES IN REAL TIME DATA
VORRICHTUNG UND VERFAHREN ZUM ERZEUGEN EINES BENUTZERDEFINIERBAREN, VIDEODARGESTELLTEN DOKUMENTS, DAS ANDERUNGEN VON ECHTZEITDATEN ANZEIGT
DISPOSITIF ET PROCEDE PERMETTANT DE CREER UN DOCUMENT AFFICHE SUR ECRAN VIDEO QUI EST DEFINI PAR L'UTILISATEUR ET QUI PRESENTE LES MODIFICATIONS APPORTEES A DES
PATENT ASSIGNEE:
TEKNEKRON SOFTWARE SYSTEMS, INC., (1187650), 530 Lytton Avenue, Suite 301 , Palo Alto, California 94301, (US), (applicant designated states: AT;BE;CH;DE;DK;ES;FR;GB;GR;IT;LI;LU;MC;NL;SE)
INVENTOR:
RISBERG, Jeffrey, Scott, 3249 Morris Drive, Palo Alto, CA 94303, (US)
SKEEN, Marion, Dale, 3826 Magnolia Drive, Palo Alto, CA 94306, (US)
BOWLES MARK, 30 Tripp Court, Woodside, California 94062, (US)
LEGAL REPRESENTATIVE:
Dupuis-Latour, Dominique et al (152552), Avocat a la Cour, Cabinet

Bardehle, Pagenberg & Partner, 45, avenue Montaigne, 75008 Paris, (FR)
PATENT (CC, No, Kind, Date): EP 564548 A1 931013 (Basic)
EP 564548 A1 931229
EP 564548 B1 970917
WO 9212488 920723
APPLICATION (CC, No, Date): EP 92902761 911220; WO 91US9811 911220
PRIORITY (CC, No, Date): US 636044 901228
DESIGNATED STATES: AT; BE; CH; DE; DK; ES; FR; GB; GR; IT; LI; LU; MC; NL; SE
INTERNATIONAL PATENT CLASS: G06F-017/60; G06F-003/033; G06F-009/44;
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9709W2	4999
CLAIMS B	(German)	9709W2	4726
CLAIMS B	(French)	9709W2	5724
SPEC B	(English)	9709W2	20481
Total word count - document A			0
Total word count - document B			35930
Total word count - documents A + B			35930

...SPECIFICATION hereby incorporated by reference. The TIB(R) software supports subject based addressing, network architecture decoupling, **communication protocol** decoupling, data decoupling and separation of information sources from consumers. The TIB software subject based...

...spreadsheet. The spreadsheet can compute a result, e.g., the theoretical value of a derivative **security** , and publish it on the network through the TIB software. The program of the invention...

...display at any particular time, but in alternative embodiments, several sheets may be shown in **separate** "windows" or **layers** on the display.

BRIEF DESCRIPTION OF THE DRAWINGS:
Figure 1 is a typical sheet layout...to the securities on the list. The ticker attributes are:
* Create (command button)

Adds a **security** to the list. A mouse click on a Create Button, i.e., the icon 19...tool is as follows:
* Market Type (list)

Used to select the Market Type for the **security** .
* Ticker Style (list)

Used to select the display format for trades or updates to the...

...styles are generally different for the different market types.
* Symbol (field)

Used to enter the **security** symbol. The same conventions are used as for entering the symbol into the Quote dialog...use the alert facility:
1. Make sure the correct price axis is highlighted for the **security** for which the user wishes to set an alert.
2. Create two trend lines that define upper and lower limit ranges (a "channel") for the **security** .
3. Activate the trend lines by clicking on any trend point with the right mouse...

...line. The right mouse button is a toggle between active and inactive.
4. If the **security** value goes above or below the channel formed by the two trend lines, the graph...market data from the Teknekron Information Bus(TM) (TIB(TM)) component, a powerful suite of **communication protocols** that **separate** information sources, like MarketFeed 2, Ticker III, or Telerate TDPF from information consumers,

like MarketSheet...clicked on. This allows the creation of "hypertext links" between related information, such as a **security** and its options pricing. Available tools include:
* Grid

When this tool is active, all creation...

9/3,K/11
DIALOG(R)File 348:European Patents

00541312
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
A method for providing a security **facility for remote systems management.**
Verfahren zur Sicherheitsanordnung fur eine Fernsystemeverwaltung.
Methode pour realiser un dispositif de securite dans le cadre de la gestion de systemes a distance.
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313080), 146 Main Street, Maynard, MA 01754, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Sudama, Ram, 14 Lake Shore Drive, Hudson, Massachusetts 01749, (US)
Griffin, David Michael, 52 Summerhill Road, Maynard, Massachusetts 01754, (US)
Johnson, Brad C., 45 Oak Street, Westerly, Rhode Island 02891, (US)
Sealy, Dexter, 650 Columbus Ave, Boston, MA 02118, (US)
Shelhamer, James, 26 Concord Street, Maynard, MA 01754, (US)
Tallman, Owen Harold, 852 Massachusetts Ave, Lunenburg, MA 01462, (US)
LEGAL REPRESENTATIVE:
Oliver, Peter Anthony (50943), BEACHCROFT STANLEYS 20 Furnival Street, London EC4A 1BN, (GB)
PATENT (CC, No, Kind, Date): EP 520709 A2 921230 (Basic)
EP 520709 A3 940824
APPLICATION (CC, No, Date): EP 92305673 920619;
PRIORITY (CC, No, Date): US 722879 910628
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: G06F-001/00; G06F-012/14;
ABSTRACT WORD COUNT: 76

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1245
SPEC A	(English)	EPABF1	6096
Total word count - document A			7341
Total word count - document B			0
Total word count - documents A + B			7341

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
A method for providing a security **facility for remote systems management.**

...ABSTRACT A2
This invention consists of a method for providing **security** for distributing management operations among components of a computer network using a network of mutually...

...SPECIFICATION invention relates to networked data processing systems, and in particular, to methods for providing a **security** facility for remote systems management (RSM). RSM consists of performing system and application management functions...

...a local system (i.e., within the control of a single management server) are executed **independently** of network **protocol** . These processes are free to manipulate local data and make local decisions. However, when processes...

...they communicate under the control of the network management servers.
The management servers implement network **communication protocol** for transferring data and requests for performance of functions by network resources between the nodes...

...management operation.
The management servers in a network should execute system management, which includes network **communication protocol** , in the networked data processing system in a way that maintains the "**security** " of the local systems and of the communication links between the local systems. Network **security** has traditionally consisted of means to protect against unauthorized access to operations or data contained within the network. This type of **security** prevents unintentional as well as deliberate attempts to access information or network processing resources within the data processing network. Another important aspect of **security** is the assurance given to the sender of data or network requests that the recipient will not corrupt or make unauthorized use of the information transmitted by the sender. "**Security** " not only consists of restricting access to network resources, but also includes the guarantee that...

...management server, a data storage system or a data processing system.
A "threat" to the **security** in a network is used herein to denote any activity which, if successful, will result in a breach of the **security** of the system.- A threat, if not neutralized, may destroy,-alter, duplicate or transmit without...

...can be created by impostors or unauthorized processes operating within the network.
Prior network management **security** facilities depend ...servers.
First, heterogenous management systems, i.e., ones containing local operating systems implementing inconsistent system **security** measures, cannot guarantee uniform protection of information transmitted between local systems in the network once the receiving management server gains control of the information. The **security** measures utilized by the receiving system may be inadequate or the receiving management server may ...

...be compromised after the receiving management server gains control of the information.
Second, some prior **security** mechanisms are not designed for RSM operations, and are not completely secure when used in...

...unauthorized access to restricted network resources or information.
In addition, locating the source of a **security** breach is difficult if each local system management server possesses the capability of utilizing programming tools outside the domain of RSM to modify the **security** measures associated with its local operating system. In order to diagnose all weak links in the **security** of the network, the local **security** measures of each management server in the network must be reviewed. Therefore, not only are these prior art systems subject to consequences of local **security** breaches, but also, the difficulty in identifying the source of the **security** breach increases as the size of the network becomes larger.
Therefore, known RSM **security** facilities which utilize local **security** mechanisms external to the management service may present significant problems to one wishing to maintain a secure network. Weak **security** measures used by a local system may not be apparent to other local operating system management servers or users who do not have information relating to the **security** measures adopted by the other local systems of the network. Identifying the source of a **security** breach is complicated in systems where non-uniform **security** rules are used by different local operating systems because diagnosis requires knowledge of each local system's **security** measures. This is a formidable task if the network consists of more than a few nodes. Furthermore, diagnosis and elimination of **security** threats is further complicated when local **security** measures may be changed outside the network operating environment by local operating systems.

Other approaches for providing **security** for RSM operations performed in a network environment depend on global user authentication. As an example, private-key **encryption** services in which keys are assigned to specific processes are frequently employed. This approach is...

...cannot be modified without permission by a network authorization procedure. However, even under these circumstances **security** is not guaranteed because management systems which permit the control of operations to span multiple...

...services to a large-scale networked computing environment, such approaches fail to adequately address the **security** problem.

The desired solution to this problem is delegation which is the transfer of authenticated...

...multiple systems.

SUMMARY OF THE INVENTION

The present invention overcomes the problems in prior art **security** facilities for networked data processing systems and maintains a secure network environment through the utilization...

...management servers in the network. The method according to the invention uses an internalized network **security** facility implementing link-wise protection of management operations transmitted between management servers in a network...

...e., that transmission between the two management servers is allowed). As an added measure of **security** , the sender and receiver are each required to authenticate the other.

Furthermore, a host withholds...

...user.

The invention in its broad form resides in a system and method for providing **security** for a data processing network having (...server. Furthermore, the current invention reduces the difficulty in detecting and eliminating threats to network **security** by centralizing control over network **security** measures and providing a uniform set of rules for providing secure transmission of information between management servers. Centralization of **security** prevents local systems from singly compromising the **security** of the entire network since access to network resources from any given management server is...

...the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present invention generally relates to a **security** facility for use in a networked data processing system. It is preferred that a network ...well known method for authenticating processes is to utilize one of the several available keybased **encryption** systems to authenticate processes. Third, the management service which actually performs the function described within...

...management operations on secure paths to other local systems in the network and maintaining the **security** of the local system 2. The management server 12 determines the proper link on which...

...between the management servers. The trusted relation lists are generated independent from execution of the **communication protocol** by an autonomous network utility. These lists, though maintained by a global procedure, would preferably ...shows an illustrative network configuration of four (4) networked systems, S1-S4 for employing the **security** facility of the present invention. Each system S contains a single management server M and...

...interface at M1 will be described in order to explain in detail the link-wise **security** measures provided by the current invention for RSM operations. The execution of a specified RSM...known acceptable means such as the key-based "Kerbesos" authentication service. System designers may prefer **encryption** based authentication schemes because unauthorized parties cannot appropriate legitimate user's keys by merely monitoring...

operation submitted by an authorized user through a trusted path through the network links. Since **security** is established on a link-wise basis, a trusted path is inferred merely by verifying...

...command was received by the host C4 through its trusted management server M3. Additionally, the **security** of network transmissions is enhanced by having the management server M3 for the second host...
...performed by host C4.
Thus there has been described herein a method for providing a **security** facility to ensure that only authorized individuals are permitted to perform or receive specific management...

...CLAIMS A2
1. A method for providing **security** for a data processing network having (i) a plurality of management servers connected by transfer...

...existence of a trusted relation with the sending management server.
2. A method for providing **security** for a data processing network having at least an originating management server for providing a...

...step of authenticating by the host the final management server.
5. A method for providing **security** for a data processing network having at least an originating management server for providing a...

...existence of a trust relation with the originating management server.
6. A method for providing **security** for a data processing network according to claim 5, including retrieving by a sending intermediate ...

...step of authenticating by the host the final management server.
10. A method for providing **security** for performing a composite operation involving a plurality of hosts on a data processing network ...

9/3,K/12
DIALOG(R)File 348:European Patents

00464516
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Abort processing in pipelined communication
Verarbeitungsabbruch in Pipeline-Kommunikationen
Interruption de traitement dans une communication du type pipeline
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313088), 146 Main Street, Maynard, Massachusetts 01745, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Gupta, Amar, 35 Woodstone Road, Northboro, Massachusetts 01532, (US)
Kempf, Mark F., 18 Carriage Lane, Stow, Massacusetts 01775, (US)
Nagpal, Hari K,, 17 Travis Drive, Framingham, Massacusetts 011701, (US)
Koning, Paul G., 4 Parker Road, Brooklin, New Hampshire 03033, (US)
LEGAL REPRESENTATIVE:
Betten & Resch (101031), Reichenbachstrasse 19, 80469 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 464566 A2 920108 (Basic)
EP 464566 A3 950215
EP 464566 B1 980902
APPLICATION (CC, No, Date): EP 91110390 910624;
PRIORITY (CC, No, Date): US 546630 900629
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-029/06;
ABSTRACT WORD COUNT: 128

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:
Available Text Language Update Word Count

CLAIMS B	(English)	9836	393
CLAIMS B	(German)	9836	368
CLAIMS B	(French)	9836	513
SPEC B	(English)	9836	11155
Total word count - document A			0
Total word count - document B			12429
Total word count - documents A + B			12429

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

...SPECIFICATION messages transmitted over networks. The following background material, under the subheadings "Computer Network Background" and "**Cryptography** Background," introduces various computer network and **cryptography** concepts and definitions. Those familiar with computer networks and **cryptography** may wish to skip these two sections.

Computer Network Background:
A computer network is simply...

...or frames, such as checksums for error detection, and packet numbers. Although the data link **layer** is primarily **independent** of the nature of the physical transmission medium, certain aspects of the data link layer...routers exchange information about the identities of the networks to which they are connected.
When **cryptography** is used to protect data transmitted over a computer network, some network devices, such as...

...the message to an adjacent LAN. As will also become apparent as this description proceeds, **cryptography** as applied to networks poses some problems that do not arise in a more conventional application of **cryptography** in point-to-point communication. When a message passes down through the various protocol layers...

...a message frame to its intended destination and to recreate the message at the destination. **Encryption** must usually be applied only to the message content and not to the various message...
...network protocols may be employed at any of the protocol levels. Therefore, a hardware-implemented **cryptographic** system for networks must be capable of handling message frames originating from these different protocols...

...frames may get segmented into smaller frames as it passes through several intermediate network links.

Cryptography Background:
The principal goal of **encryption** is to render communicated data secure from unauthorized eavesdropping. This is generally referred to as the "secrecy" or "confidentiality" requirement of **cryptographic** systems. A related requirement is the "authenticity" or "integrity" requirement, which ensures that the communicated...

...Plaintext" is used to refer to a message before encrypting and after decrypting by a **cryptographic** system. "Ciphertext" is the form that the encrypted part of the message takes during transmission over a communications channel. "**Encryption** " or "encipherment" is the process of transformation from plaintext to ciphertext. "**Decryption** " or "decipherment" is the process of transformation from ciphertext to plaintext. Both **encryption** and **decryption** are controlled by a "cipher key," or keys. Without knowledge of the **encryption** key, a message cannot be encrypted, even with knowledge of the encrypting process. Similarly, without knowledge of the **decryption** key, the message cannot be decrypted, even with knowledge of the decrypting process.
More specifically, a **cryptographic** system can be thought of as having an enciphering transformation Ek)), which is defined by...

...Ek)) encrypts a plaintext message M into an encrypted message, or ciphertext C. Similarly, the **decryption** is performed by a

non-SNAP/SAP destination. This case...

...statistics. Such flexibility for selective disclosure of the protocol can be of great importance in **security** and network management.
It will be understood that the foregoing description includes, by way of...

...invention may be readily adapted for use in an Ethernet network architecture. Further, although the **cryptography** processing described above is best implemented in an "on-board" processor that is integrated physically with other conventional network processing components, the principles of the invention still apply when the **cryptographic** processing is performed by an "off-board" processor or device added to a conventional network processor or node that did not previously have **cryptographic** capability.
It will be appreciated that the present invention represents a significant improvement in the...

...CLAIMS in claim 1, wherein:

one of the first, second and third processing modules is a **cryptographic** processor for performing in-line **encryption** and **decryption** of information packets transmitted onto and received from a communication network.
4. A method for...

...defined in claim 4, wherein:

one of the first and second processing modules is a **cryptographic** processor for performing in-line **encryption** and **decryption** of information packets transmitted onto and received from a communication network.
...CLAIMS dans lequel :

l'un des premier, second et troisieme modules de traitement est en processeur **cryptographique** pour assurer le chiffrement et le dechiffrement direct de paquets d'informations transmis sur un...

...4, dans lequel:

l'un des premier et second modules de traitement est un processeur **cryptographique** pour le chiffrement et le dechiffrement direct de paquets d'informations transmis sur un reseau...

9/3,K/13
DIALOG(R)File 348:European Patents

00464515
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Cryptography **processor and method with optional status encoding.**
Krypto-Prozessor und Verfahren mit wahlweiser Statuskodierung.
Processeur cryptographique **et procede avec codage d'etat facultatif.**
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313088), 146 Main Street, Maynard, Massachusetts 01745, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Gupta, Amar, 35 Woodstone Road, Northboro, Massachusetts 01532, (US)
Hawe, William R., 16 Independence Road, Pepperell, Massachusetts 01463, (US)
Kempf, Mark F., 18 Carriage Lane, Stow, Massachusetts 01775, (US)
Lee, Ching Shui, 166 Oak Street, Ashland, Massachusetts 01721, (US)
Lampson, Butler W., 180 Lakeview Avenue, Cambridge, Massachusetts 02138, (US)
Spinney, Barry A., 22 Anthony Road, Wayland, Massachusetts 01778, (US)

Tardo, Joseph J., 6 Trask Road, Acton, Massachusetts, (US)
Kaufman, Charles W., 185 Indian Meadow Drive, Northboro, Massachusetts, (US)
Herbison, B. J., 18 Drummer Lane, Leominster, Massachusetts, (US)
Gasser, Morrie, 11 Golden Hills Road, Saugus, Massachusetts, (US)
LEGAL REPRESENTATIVE:
Betten & Resch (101031), Reichenbachstrasse 19, W-8000 Munchen 5, (DE)
PATENT (CC, No, Kind, Date): EP 464565 A2 920108 (Basic)
EP 464565 A3 930526
APPLICATION (CC, No, Date): EP 91110389 910624;
PRIORITY (CC, No, Date): US 546631 900629; US 546614 900629; US 546632 900629
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-029/02; H04L-009/00;
ABSTRACT WORD COUNT: 169

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1681
SPEC A	(English)	EPABF1	11896
Total word count - document A			13577
Total word count - document B			0
Total word count - documents A + B			13577

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

Cryptography **processor and method with optional status encoding.**
Processeur cryptographique **et procede avec codage d'etat facultatif.**

...ABSTRACT A2

Cryptographic apparatus, and a related method for its operation, for in-line **encryption** and **decryption** of data packets transmitted in a communication network. A full-duplex **cryptographic** processor is positioned between two in-line processing entities of a network architecture. For example...

...decide whether or not they contain encrypted data and, if they do, are subject to **decryption** before forwarding. Outbound information packets have their data portions encrypted if called for, and are usually forwarded toward the network communication medium. **Cryptographic** processing in both directions is performed in real time as each packet is streamed through...

...processed information back in a reverse direction, to permit the host system to perform local **encryption** or **decryption** for various purposes. (see image in original document)
...SPECIFICATION messages transmitted over networks. The following background material, under the subheadings "Computer Network Background" and "**Cryptography** Background," introduces various computer network and **cryptography** concepts and definitions. Those familiar with computer networks and **cryptography** may wish to skip these two sections.
Computer Network Background:
A computer network is simply...

...or frames, such as checksums for error detection, and packet numbers.
Although the data link **layer** is primarily **independent** of the nature of the physical transmission medium, certain aspects of the data link layer...routers exchange information about the identities of the networks to which they are connected.
When **cryptography** is used to protect data transmitted over a computer network, some network devices, such as...

...the message to an adjacent LAN. As will also become apparent as this description proceeds, **cryptography** as applied to networks poses some problems that do not arise in a more conventional application of **cryptography** in point-to-point communication. When a message passes down through the various protocol layers...
...a message frame to its intended destination and to recreate the message

16. A method of operation of **cryptographic** apparatus in a communication network having multiple node processors connected to communication medium, the method...

...from the content of the packet received from the second interface whether or not to **cryptographically** process data within the packet;
cryptographically processing data in the transmittable packet if necessary; and
forwarding the processed packet.
18. A...

9/3,K/14
DIALOG(R)File 348:European Patents
(c) 1998 European Patent Office. All rts. reserv.

00464514
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Generic encryption **technique for communication networks**
Allgemeines Verschlusselungsverfahren fur Kommunikationsnetze
Procede general de chiffrage pour reseaux de communication
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313088), 146 Main Street, Maynard, Massachusetts 01745, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Hawe, William R., 16 Independence Road, Pepperell, Massachusetts 01463, (US)
Tardo, Joseph J., 6 Trask Road, Acton, Massachusetts 01720, (US)
Kaufman, Charles W., 185 Indian Meadow Drive, Northboro, Massachusetts 01532, (US)
Gupta, Amar, 35 Woodstone Road, Northboro, Massachusetts 01532, (US)
Spinney, Barry A., 22 Anthony Road, Wayland, Massachusetts 01778, (US)
Waters, Gregory M., 15 Park Drive No. 27, Boston, Massachusetts 02215, (US)
LEGAL REPRESENTATIVE:
Betten & Resch (101031), Reichenbachstrasse 19, D-80469 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 464564 A2 920108 (Basic)
EP 464564 A3 921125
EP 464564 B1 960403
APPLICATION (CC, No, Date): EP 91110388 910624;
PRIORITY (CC, No, Date): US 546629 900629
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-029/06; H04L-009/00;
ABSTRACT WORD COUNT: 194

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	908
CLAIMS B	(English)	EPAB96	907
CLAIMS B	(German)	EPAB96	819
CLAIMS B	(French)	EPAB96	1011
SPEC A	(English)	EPABF1	11840
SPEC B	(English)	EPAB96	11807
Total word count - document A			12748
Total word count - document B			14544
Total word count - documents A + B			27292

ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Generic encryption **technique for communication networks**

...ABSTRACT A2
A method and related **cryptographic** processing apparatus for handling information packets that are to be **cryptographically** processed prior to transmission onto a communication network, or that are to be locally **cryptographically** processed and looped back to a node processor. A special **cryptographic** preamble is included in each information packet

that is to be subject to **cryptographic** processing. The **cryptographic** preamble contains an offset value pointing to the starting location of information that is to be processed, and completely defines the type of **cryptographic** processing to be performed. The **cryptographic** processor can then perform the processing as specified in the preamble without regard to a...

...is to be transmitted onto the network, the preamble is stripped from the packet after **cryptographic** processing, so that the formats of packets transmitted onto the network will be unaffected by the preamble. **Cryptographic** processing modes include **encryption** of data for outbound transmission, **encryption** of a cipher key for loopback to the node processor, **encryption** or **decryption** of data for loopback to the node processor, and computation of an integrity check value...

...SPECIFICATION messages transmitted over networks. The following background material, under the subheadings "Computer Network Background" and "**Cryptography** Background," introduces various computer network and **cryptography** concepts and definitions. Those familiar with computer networks and **cryptography** may wish to skip these two sections.

Computer Network Background:

A computer network is simply...

...or frames, such as checksums for error detection, and packet numbers.

Although the data link **layer** is primarily **independent** of the nature of the physical transmission medium, certain aspects of the data link layer...routers exchange information about the identities of the networks to which they are connected.

When **cryptography** is used to protect data transmitted over a computer network, some network devices, such as...

...the message to an adjacent LAN. As will also become apparent as this description proceeds, **cryptography** as applied to networks poses some problems that do not arise in a more conventional application of **cryptography** in point-to-point communication. When a message passes down through the various protocol layers...

...a message frame to its intended destination and to recreate the message at the destination. **Encryption** must usually be applied only to the message content and not to the various message...

...network protocols may be employed at any of the protocol levels. Therefore, a hardware-implemented **cryptographic** system for networks must be capable of handling message frames originating from these different protocols...

...frames may get segmented into smaller frames as it passes through several intermediate network links.

Cryptography Background:

The principal goal of **encryption** is to render communicated data secure from unauthorized eavesdropping. This is generally referred to as the "secrecy" or "confidentiality" requirement of **cryptographic** systems. A related requirement is the "authenticity" or "integrity" requirement, which ensures that the communicated...

...Plaintext" is used to refer to a message before encrypting and after decrypting by a **cryptographic** system. "Ciphertext" is the form that the encrypted part of the message takes during transmission over a communications channel. "**Encryption** " or "encipherment" is the process of transformation from plaintext to ciphertext. "**Decryption** " or "decipherment" is the process of transformation from ciphertext to plaintext. Both **encryption** and **decryption** are controlled by a "cipher key," or keys. Without knowledge of the **encryption** key, a message cannot be encrypted, even with knowledge of the encrypting process. Similarly, without knowledge of the **decryption** key, the message cannot be decrypted, even with knowledge of the decrypting process.

More specifically, a **cryptographic** system can be thought of as having an enciphering transformation E(sub(k)), which is...

cryptographic preamble that is attached to the message packet when **encryption** is desired. The **cryptographic** preamble contains **encryption** key information and an offset (i.e. a pointer) indicating the starting point in the packet at which **encryption** is to begin. Thus the **cryptographic** processor can skip intervening header information, regardless of its format and protocol, and begin **encryption** at the location indicated by the **cryptographic** header. The header does not affect packet formats transmitted on a network, because it (the **cryptographic** header) is stripped off the packet prior to transmission. Basically, this feature of the invention...

...of falsely encrypted packets onto the network. It also greatly simplifies the implementation of the **cryptographic** processor, since each packet does not have to be completely parsed or analyzed to find the location of the data to be encrypted.

The **cryptographic** preamble in a presently preferred embodiment of the invention is in the following format: (see...

...a 12-bit offset that indicates the number of bytes to skip before starting the **cryptographic** operation. The flag bits include a device specific bit that will be zero in most cases, and a three-bit mode field that indicates the type of **encryption** operation being performed. The mode may be:

0: Outbound **encryption** (not a loopback);
1: Loopback KEY **encryption** ;
2: Loopback **encryption** ;
3: Loopback **decryption** ;
4: Loopback ICV only.

The SE-CTRL field defines the type of **cryptographic** process, and has fields to indicate confidentiality **encryption** , integrity **encryption** , the type of **cryptographic** algorithm (DES or other), the specific **cryptographic** algorithm mode used (such as ECB, CFB or CBC), and the size of the cyclic...

...CRC) to be used. The transmit key is an 8-byte field that defines the **cryptographic** key used for **encryption** .

The **cryptographic** preamble contains all the information needed to locate the data that is to be encrypted and to determine the type of **encryption** that is required, regardless of the packet format that is used by various protocols. Use of the **cryptographic** preamble prevents the transmission of falsely encrypted packets onto the network. In addition, the presence of the preamble simplifies the hardware needed for **encryption** , since the entire packet does not need to be parsed.

Use of programmable registers to facilitate **decryption** :

In the **cryptographic** processing of received packets, the basic information needed includes the location of the decrypted data within the packet, and control for the **decryption** to be performed, such as the **decryption** key and the mode of **encryption** . The **cryptographic** preamble discussed above is not available at the receiving end of a transmission, since it...

...transmission onto the network.

This situation is complicated by the fact

Status: Break Sent.

?t 9/5/15-20;t 11/5/1-2;t 12/5/1-12

9/5/15

DIALOG(R)File 348:European Patents

00464512

Encryption **with selective disclosure of protocol identifiers**

Verschlusselung mit selektiver Bekanntgabe der Protokollkennungen

Chiffrage avec revelation selective d'identificateurs de protocole

PATENT ASSIGNEE:

DIGITAL EQUIPMENT CORPORATION, (313088), 146 Main Street, Maynard,

Massachusetts 01745, (US), (applicant designated states: DE;FR;GB;IT;NL)

INVENTOR:
Gupta, Amar, 35 Woodstone Road, Northboro, Massachusetts 01532, (US)
Kaufman, Charles W., 185 Indian Meadow Drive, Northboro, Massachusetts 01532, (US)
Koning, G. Paul, 4 Parker Road, Brookline, New Hampshire 03033, (US)

LEGAL REPRESENTATIVE:
Betten & Resch (101031), Reichenbachstrasse 19, 80469 Munchen, (DE)

PATENT (CC, No, Kind, Date): EP 464563 A2 920108 (Basic)
EP 464563 A3 921104
EP 464563 B1 970423

APPLICATION (CC, No, Date): EP 91110386 910624;

PRIORITY (CC, No, Date): US 546615 900629

DESIGNATED STATES: DE; FR; GB; IT; NL

INTERNATIONAL PATENT CLASS: H04L-029/06

CITED REFERENCES (EP A):
IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION. vol. 8, no. 1, January 1990, NEW YORK US pages 42 - 48; G.VARGHESE ET AL: 'TRANSPARENT INTERCONNECTION OF INCOMPATIBLE LOCAL AREA NETWORKS USING BRIDGES'
CCITT RECOMMENDATION X.509 vol. VIII, no. 8, 14 November 1988, MELBOURNE, AU 'DATA COMMUNICATION NETWORKS: THE DIRECTORY AUTHENTICATION FRAMEWORK';

ABSTRACT EP 464563 A2

A method for selective disclosure of the identity of a **communication protocol** under which an information packet originated, but without incorrectly identifying the protocol in a header accompanying the packet. If there is a need to conceal the identity of the underlying source protocol, a special anonymous protocol identifier is used, instead of the real protocol identifier, in the header of an encrypted information packet. Network monitors can then still provide accurate information concerning traffic on the network, without having this information distorted by the use of incorrect **communication protocols** . If there is a desire to reveal the underlying protocol, a subnetwork protocol frame format is used to store the protocol identity and signify whether the packet is encrypted. A packet that is of a non-subnetwork protocol can be encapsulated with a subnetwork header containing a special code signifying that there is an encapsulated packet and containing the original protocol identifier.

ABSTRACT WORD COUNT: 153

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	920108	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	920108	A2	Date of filing of request for examination: 910724
Search Report:	921104	A3	Separate publication of the European or International search report
Examination:	950419	A2	Date of despatch of first examination report: 950307
Grant:	970423	B1	Granted patent
Change:	971203	B1	Rectifications of patent applications (change)
Oppn None:	980415	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	409
CLAIMS B	(English)	EPAB97	373
CLAIMS B	(German)	EPAB97	321
CLAIMS B	(French)	EPAB97	437
SPEC A	(English)	EPABF1	11590
SPEC B	(English)	EPAB97	11522
Total word count - document A			12000
Total word count - document B			12653
Total word count - documents A + B			24653

9/5/16
DIALOG(R)File 348:European Patents

00464511
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Method and apparatus for decryption **of an information packet having a format subject to modification**
Verfahren und Einrichtung zur Entschlusselung eines Informationspakets mit einem modifizierbaren Format
Procede et dispositif de dechiffrage d'un paquet d'informations ayant un format sujet a des modifications
PATENT ASSIGNEE:
DIGITAL EQUIPMENT CORPORATION, (313088), 146 Main Street, Maynard, Massachusetts 01745, (US), (applicant designated states: DE;FR;GB;IT;NL)
INVENTOR:
Hawe, William R., 16 Independence Road, Pepperell, Massachusetts 01463, (US)
Lampson, Butler W., 180 Lakeview Avenue, Cambridge, Massachusetts 02138, (US)
Gupta, Amar, 35 Woodstone Road, Northboro, Massachusetts 01532, (US)
LEGAL REPRESENTATIVE:
Betten & Resch (101031), Reichenbachstrasse 19, 80469 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 464562 A2 920108 (Basic)
EP 464562 A3 921104
EP 464562 B1 970423
APPLICATION (CC, No, Date): EP 91110385 910624;
PRIORITY (CC, No, Date): US 546628 900629
DESIGNATED STATES: DE; FR; GB; IT; NL
INTERNATIONAL PATENT CLASS: H04L-029/06;
CITED PATENTS (EP A): EP 289248 A; EP 279232 A; GB 2200818 A
CITED REFERENCES (EP A):
CCITT RECOMMENDATION X.509 vol. VIII, no. 8, 14 November 1988, MELBOURNE, AU 'DATA COMMUNICATION NETWORKS: THE DIRECTORY AUTHENTICATION FRAMEWORK';

ABSTRACT EP 464562 A2
A technique to facilitate **decryption** processing of information packets transmitted over a communication network after **encryption** in accordance with a specific network protocol, the details of which may be subject to later change as standards are developed or modified. Programmable registers are used in the **decryption** process to hold information for identifying an incoming information packet as being subject to the specific protocol and requiring **decryption** , and identifying a starting location of a data field to be decrypted. Specifically one programmable register contains a first offset locating an identifier field in the packet, in which a **cryptographic** identifier will be found if the packet is one conforming to the protocol; another programmable register contains a **cryptographic** identifier value that will be found in the identifier field if **decryption** is to be performed, and a third programmable register contains a second offset to locate the beginning of a data field to be decrypted. (see image in original document)
ABSTRACT WORD COUNT: 159

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	920108	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	920108	A2	Date of filing of request for examination: 910724
Search Report:	921104	A3	Separate publication of the European or International search report
Examination:	950419	A2	Date of despatch of first examination report: 950307
Grant:	970423	B1	Granted patent

Oppn None: 980415 B1 No opposition filed
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	479
CLAIMS B	(English)	EPAB97	475
CLAIMS B	(German)	EPAB97	475
CLAIMS B	(French)	EPAB97	538
SPEC A	(English)	EPABF1	11639
SPEC B	(English)	EPAB97	11626
Total word count - document A			12117
Total word count - document B			13114
Total word count - documents A + B			25231

9/5/17
DIALOG(R)File 348:European Patents

00318603
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Digital key telephone system
Digitales Tastengegensprechsystem
Systeme telephonique numerique a touches
PATENT ASSIGNEE:
NORTHERN TELECOM LIMITED, (217325), World Trade Center of Montreal, 380 St. Antoine Street West 8th Floor, Montreal, Quebec H2Y 3Y4, (CA), (applicant designated states: AT;BE;DE;ES;FR;GB;IT;NL;SE)
INVENTOR:
Nizamuddin, Nadir, 39 Chickasaw Crescent, Kanata, Ontario K2M 1M6, (CA)
Williams, John William Joseph, 18 Banting Crescent, Kanata, Ontario, K2K 1P4, (CA)
Redmond, Alan Morris, 57 Shetland Way, Kanata, Ontario, K2M 1S4, (CA)
Morley, Robert Samuel, 304 Somerset Street East, Ottawa, Ontario K1N 6W1, (CA)
Robertson, David Joseph, 161 Mulvihill Avenue, Ottawa, Ontario K1Y 6Y3, (CA)
Maginley, Ronald James, 123 Fieldcrest Street, Apt. 204,, Ann Arbor, Michigan, (US)
Chapman, Alan Stanley John, 50 Pentland Crescent, Kanata, Ontario K2K 1V5, (CA)
Thomas, Terence Neil, 6 Kelowna Street, Nepean,, Ontario K2C 3H2, (CA)
LEGAL REPRESENTATIVE:
Dennis, Mark Charles et al (30074), Nortel Limited Patents and Licensing West Road, Harlow Essex CM20 2SH, (GB)
PATENT (CC, No, Kind, Date): EP 331838 A2 890913 (Basic)
EP 331838 A3 900530
EP 331838 B1 930310
APPLICATION (CC, No, Date): EP 88310693 881111;
PRIORITY (CC, No, Date): US 166345 880310
DESIGNATED STATES: AT; BE; DE; ES; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS: H04M-009/00
CITED PATENTS (EP A): WO 8501855 A; US 4363936 A; US 4292474 A; GB 2047048 A

ABSTRACT EP 331838 A2
A key telephone system includes a plurality of ports being linked by port associated bidirectional communication channels which are synchronously switched by transferring bit states between ones of the channels to provide communication paths between the ports as directed by a central processor (7). The ports are also linkable to and via the central processor (7) by port associated message channels. An interface circuit (8) is responsive to the central processor and message channel signals for regulating flow of messages received by the central processor and for effecting single and plural channel distribution of messages from the central processor (7). The message channels permit telephony operating features and functions to be provided either within the central

processor or by appropriate apparatus means being connected at any of the ports.
ABSTRACT WORD COUNT: 133

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	890913	A2	Published application (Alwith Search Report ;A2without Search Report)
Search Report:	900530	A3	Separate publication of the European or International search report
Examination:	900816	A2	Date of filing of request for examination: 900612
Change:	910918	A2	Representative (change)
Examination:	911113	A2	Date of despatch of first examination report: 910927
*Assignee:	921007	A2	Applicant (transfer of rights) (change): NORTHERN TELECOM LIMITED (217325) World Trade Center of Montreal, 380 St. Antoine Street West, 8th Floor Montreal, Quebec H2Y 3Y4 (CA) (applicant designated states: AT;BE;DE;ES;FR;GB;IT;NL;SE)
Grant:	930310	B1	Granted patent
Oppn:	940209	B1	Opposition 01/931210 Alcatel N.V.; Strawinskykaan 341; NL-1077 XX AMSTERDAM; (NL) (Representative:)Graf, Georg Hugo, Dipl.-Ing.; Alcatel SEL AG Patent- und Lizenzwesen Postfach 30 09 29; D-70449 Stuttgart; (DE)
Change:	940309	B1	Representative (change)
Change:	940803	B1	Representative (change)
Lapse:	941207	B1	Date of lapse of the European patent in a Contracting State: BE 931130
Lapse:	950222	B1	Date of lapse of the European patent in a Contracting State: BE 931130, FR 940729
Lapse:	950308	B1	Date of lapse of the European patent in a Contracting State: BE 931130, FR 940729, NL 940601
Amended:	960612	B2	Maintenance of the European patent as amended

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPAB96	1011
CLAIMS B	(German)	EPAB96	831
CLAIMS B	(French)	EPAB96	1115
SPEC B	(English)	EPAB96	9170
Total word count - document A			0
Total word count - document B			12127
Total word count - documents A + B			12127

9/5/18
DIALOG(R)File 348:European Patents

00282751
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
INPUT/OUTPUT NETWORK FOR COMPUTER SYSTEM.
EINGANGS/AUSGANGSNETZ FUR EIN RECHNERSYSTEM.
RESEAU D'ENTREE/SORTIE POUR UN SYSTEME D'ORDINATEURS.
PATENT ASSIGNEE:
Datapoint Corporation, (290460), 9725 Datapoint Drive, San Antonio Texas 78284, (US), (applicant designated states: AT;BE;CH;DE;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
FISCHER, Michael, A., 2910 Hunter's Horn, San Antonio, TX 78230, (US)
LEGAL REPRESENTATIVE:
Waxweiler, Jean et al (19251), Dennemeyer & Associates Sarl P.O. Box 1502 , L-1015 Luxembourg, (LU)
PATENT (CC, No, Kind, Date): EP 333715 A1 890927 (Basic)

EP 333715 A1 910130
EP 333715 B1 931201
WO 8804511 880616
APPLICATION (CC, No, Date): EP 87906702 870918; WO 87US2388 870918
PRIORITY (CC, No, Date): US 941084 861212
DESIGNATED STATES: AT; BE; CH; DE; FR; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: H04Q-009/00; H04J-003/24; G06F-013/00;
CITED PATENTS (WO A): US 4423414 A; US 4495493 A; US 4549297 A; US 4574284 A; US 4680581 A; US 4692918 A; US 4706080 A
CITED REFERENCES (EP A):
No further relevant documents have been disclosed.
See also references of WO8804511;
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	890927 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	890927 A1	Date of filing of request for examination: 890612
Search Report:	910130 A1	Drawing up of a supplementary European search report: 901214
Examination:	920422 A1	Date of despatch of first examination report: 920305
Grant:	931201 B1	Granted patent
Change:	940831 B1	Representative (change)
Lapse:	940928 B1	Date of lapse of the European patent in a Contracting State: NL 931201
Lapse:	941026 B1	Date of lapse of the European patent in a Contracting State: NL 931201, SE 931201
Lapse:	941117 B1	Date of lapse of the European patent in a Contracting State: AT 931201, NL 931201, SE 931201
Oppn None:	941123 B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	2844
CLAIMS B	(German)	EPBBF1	2410
CLAIMS B	(French)	EPBBF1	3383
SPEC B	(English)	EPBBF1	20008
Total word count - document A			0
Total word count - document B			28645
Total word count - documents A + B			28645

9/5/19
DIALOG(R)File 348:European Patents

00211276
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Alternate routing arrangement.
Umweglenkungsanordnung.
Agencement pour acheminement alternatif.
PATENT ASSIGNEE:
AMERICAN TELEPHONE AND TELEGRAPH COMPANY, (589370), 550 Madison Avenue, New York, NY 10022, (US), (applicant designated states: DE;FR;GB;IT;NL;SE)
INVENTOR:
Olson, Jeffrey James, 5512 La Plata Circle, Boulder Colorado 80301, (US)
Peck, Stephen Richard, 4410 Lariat Way, Boulder Colorado 80301, (US)
Seaton, David Paul, 1525 Harrison Avenue, Boulder Colorado 80303, (US)
LEGAL REPRESENTATIVE:
Blumbach Weser Bergen Kramer Zwirner Hoffmann Patentanwalte , Sonnenbergerstrasse 43, D-6200 Wiesbaden 1, (DE)
PATENT (CC, No, Kind, Date): EP 224229 A2 870603 (Basic)
EP 224229 A3 890628
APPLICATION (CC, No, Date): EP 86116227 861122;
PRIORITY (CC, No, Date): US 802573 851127

DESIGNATED STATES: DE; FR; GB; IT; NL; SE
INTERNATIONAL PATENT CLASS: H04L-011/20;
CITED PATENTS (EP A): US 4287592 A; US 4287592 A; JP 60177754 A; WO 8502737 A; JP 60177761 A
CITED REFERENCES (EP A):
PATENT ABSTRACTS OF JAPAN, vol. 8, no. 8 (E-221) 1445 , 13th January 1984; & JP-A-58 175 343 (NIPPON DENKI K.K.) 14-10-1983
Idem;

ABSTRACT EP 224229 A2
Improved alternate routing in a packet switching system is provided by inserting alternate routing control information (FIG. 11) into each packet and by storing alternate routing information at each network node (A, B, C). The stored information at each node (A, B, C) includes a list of the available paths (107, 108, 109) extending from the node towards all other nodes together with a list of available algorithms that can be used to select one of the available routes. The alternate routing control information (ARF) in each packet contains postage information specifying the maximum number of nodes through which the packet is to travel. The alternate routing control information (ARF) also includes a destination map index code identifying the destination node. The destination map index is used as address information by each node receiving a packet to read out the stored information at the node identifying the available paths and the algorithm to be used in selecting one of these paths for use in transmitting the packet towards the destination node. The identified algorithm is then executed to select the path to be used.
ABSTRACT WORD COUNT: 188

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	870603	A2	Published application (A1with Search Report ;A2without Search Report)
Change:	890614	A2	Obligatory supplementary classification (change)
Search Report:	890628	A3	Separate publication of the European or International search report
Withdrawal:	891115	A2	Date on which the European patent application was withdrawn: 890920

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	2699
SPEC A	(English)	EPABF1	14572
Total word count - document A			17271
Total word count - document B			0
Total word count - documents A + B			17271

9/5/20
DIALOG(R)File 348:European Patents

00172351
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Interface process for an all points addressable printer.
Schnittstellenverfahren fur allpunktadressierbaren Drucker.
Procede d'interface pour imprimante a tous points adressables.
PATENT ASSIGNEE:
International Business Machines Corporation, (200120), Old Orchard Road, Armonk, N.Y. 10504, (US), (applicant designated states: BE;CH;DE;FR;GB;IT;LI;NL;SE)
INVENTOR:
Herzog, Alexander, 4786 Kellog Circle, Boulder Colorado 80303, (US)
Marlin, James Warden, 5939 Niwot Road, Longmont Colorado 80501, (US)
Platte, Brian Gerald, Sugarloaf Star Route, Boulder Colorado 80302, (US)
Yeskel, Filip Jay, 147, Cherokee Way, Boulder Colorado 80303, (US)
LEGAL REPRESENTATIVE:
Schuffenecker, Thierry (69981), Compagnie IBM France, Departement de

Propriete Intellectuelle, F-06610 La Gaude, (FR)
PATENT (CC, No, Kind, Date): EP 191177 A2 860820 (Basic)
EP 191177 A3 891115
EP 191177 B1 940608
APPLICATION (CC, No, Date): EP 85115709 851210;
PRIORITY (CC, No, Date): US 700427 850211
DESIGNATED STATES: BE; CH; DE; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: G06F-003/12;
CITED PATENTS (EP A): WO 8301521 A; EP 123109 A
CITED REFERENCES (EP A):
NATIONAL TELECOMMUNICATIONS CONFERENCE, New Orleans, Louisiana, 29th November - 3rd December 1981, pages E4.2.1-E4.2.5, IEEE, New York, US; A.W. MAHOLICK et al.: "A communication structure for printer control"
PATENT ABSTRACTS OF JAPAN, vol. 7, no. 26 (P-172) 1171 , 2nd February 1983; & JP-A-5 178523 (MITSUBISHI DENKI K.K.) 02-11-1982;

ABSTRACT EP 191177 A2

This invention is a process for interconnecting an all points addressable printer (181) with a host application program (10) wherein the application presents output to be printed to the printer and wherein the host application can be present on a variety of different computing equipment such as a large host computer, a standalone workstation, or workstation on a local area network and wherein the all points addressable page printer can utilize any type of printing technology such as electrophotographic, magnetic or other and wherein the printer and the application host are interconnected by communicating means (17) such as a channel, local area network, or telecommunication line and wherein any type of transmission protocol can be used and wherein the process enables the transmission of commands and data from the host application to the printer in a manner which is independent of the communication means and transmission protocol. And, finally, wherein the process enables the transmission of a variety of types of data including text, graphics, image, or bar code which may be merged together on a single printed page.

ABSTRACT WORD COUNT: 183

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	860820	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	870204	A2	Date of filing of request for examination: 861212
Search Report:	891115	A3	Separate publication of the European or International search report
Examination:	920617	A2	Date of despatch of first examination report: 920506
Change:	921230	A2	Representative (change)
Grant:	940608	B1	Granted patent
Lapse:	950201	B1	Date of lapse of the European patent in a Contracting State: SE 940908
Lapse:	950322	B1	Date of lapse of the European patent in a Contracting State: BE 940608, SE 940908
Lapse:	950329	B1	Date of lapse of the European patent in a Contracting State: BE 940608, NL 940608, SE 940908
Oppn None:	950531	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPBBF1	2199
CLAIMS B	(English)	EPBBF1	2200
CLAIMS B	(German)	EPBBF1	2041
CLAIMS B	(French)	EPBBF1	2652
SPEC A	(English)	EPBBF1	28558
SPEC B	(English)	EPBBF1	28197
Total word count - document A			30757
Total word count - document B			35090
Total word count - documents A + B			65847

11/5/1
DIALOG(R)File 348:European Patents

00632906
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348

System and method for high speed encryption using multiple keystream generator.

System und Verfahren zur schnellen Verschlusselung unter Verwendung eines Vielfachschlusselgenerators.

Systeme et procede pour le chiffrage a grande vitesse utilisant un generateur de sequence de cle multiple.

PATENT ASSIGNEE:
Hughes Aircraft Company, (214913), 7200 Hughes Terrace P.O. Box 45066, Los Angeles, California 90045-0066, (US), (applicant designated states: DE;FR;GB)
INVENTOR:
Bianco, Mark E., 1770 Del Prado, Pomona, California 91768, (US)
Mayhew, Gregory L., P.O. Box 2346, Fullerton, California 92633, (US)
LEGAL REPRESENTATIVE:
Patentanwalte Grunecker, Kinkeldey, Stockmair & Partner (100721), Maximilianstrasse 58, D-80538 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 615361 A1 940914 (Basic)
APPLICATION (CC, No, Date): EP 94103796 940311;
PRIORITY (CC, No, Date): US 30687 930312
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-009/18; H04L-009/06;

ABSTRACT EP 615361 A1
A general purpose, high-speed encryption system (50) and method, based on a linear feedback shift register (LFSR) (70) that provides inputs to one or more mathematically independent nonlinear output functions (80A-80N), resulting in the generation of multiple keystream outputs per clock cycle. Due to the parallel architecture, the system need only operate at a rate of 1/N, where N is the number of output functions. For example, the system can encrypt an 8-bit byte in one-eighth the time required for a conventional bit-oriented stream cipher. Alternatively, with high-speed serial-to-parallel and parallel-to-serial interface converters, the system can encrypt a serial data stream at a rate N times that of the system itself. (see image in original document)
ABSTRACT WORD COUNT: 118

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	940914 A1	Published application (A1with Search Report ;A2without Search Report)
Change:	940921 A1	Inventor (change)
Examination:	950503 A1	Date of filing of request for examination: 950307
*Assignee:	981028 A1	Applicant (transfer of rights) (change): HE HOLDINGS, INC. (2459551) 7200 Hughes Terrace P.O. Box 45066 Los Angeles, California 90045-0066 (US) (applicant designated states: DE;FR;GB)
*Assignee:	981028 A1	Previous applicant in case of transfer of rights (change): Hughes Aircraft Company (214913) 7200 Hughes Terrace P.O. Box 45066 Los Angeles, California 90045-0066 (US) (applicant designated states: DE;FR;GB)
*Assignee:	981104 A1	Applicant (transfer of rights) (change): Hughes Electronics Corporation (2464050) 200N. Sepulveda Boulevard El Segundo, California 90245-0956 (US) (applicant designated states: DE;FR;GB)
*Assignee:	981104 A1	Previous applicant in case of transfer of rights (change): HE HOLDINGS, INC. (2459551) 7200 Hughes Terrace P.O. Box 45066 Los Angeles,

California 90045-0066 (US) (applicant designated states: DE;FR;GB)
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF2	675
SPEC A	(English)	EPABF2	3791
Total word count - document A			4466
Total word count - document B			0
Total word count - documents A + B			4466

11/5/2
DIALOG(R)File 348:European Patents

00592527
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Cryptographic key management method
Verfahren zur Verwaltung eines Geheimubertragungsschlussels
Procede d'administration d'une cle cryptographique
PATENT ASSIGNEE:
MOTOROLA, INC., (205770), 1303 East Algonquin Road, Schaumburg, IL 60196, (US), (applicant designated states: AT;CH;DE;DK;FR;GB;IE;IT;LI;NL;SE)
INVENTOR:
Barney, George M., 8426 E. Cholla, Scottsdale, Arizona 85260, (US)
Hardy, Douglas A., 2207 E, Gable Avenue, Mesa, Arizona 85204, (US)
Balogh, Craig R., 838 E. Harmony Avenue, Mesa, Arizona 85204, (US)
LEGAL REPRESENTATIVE:
Hudson, Peter David et al (52403), Motorola, European Intellectual Property, Midpoint, Alencon Link, Basingstoke, Hampshire RG21 7PL, (GB)
PATENT (CC, No, Kind, Date): EP 602335 A2 940622 (Basic)
EP 602335 A3 950125
EP 602335 B1 980909
APPLICATION (CC, No, Date): EP 93115876 931001;
PRIORITY (CC, No, Date): US 991054 921215
DESIGNATED STATES: AT; CH; DE; DK; FR; GB; IE; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: H04L-009/08; H04L-009/00;

ABSTRACT EP 602335 A2
A method for establishing a secure communications link between first (103, 380) and second (109, 390) terminals includes a step of exchanging (210) a first message. The first message contains information describing encryption devices and communications modes available within the terminals and user authentication information. The method also includes a step of selecting (219, 221, 222, 224), in at least one terminal (103, 109), a common key generation and ciphering algorithm. The method further includes steps of exchanging (230) a second message for providing data to form traffic keys, exchanging (250) a third message for synchronizing secure communications and initiating (270) secure communication. (see image in original document)
ABSTRACT WORD COUNT: 110

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	940622	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	950125	A3	Separate publication of the European or International search report
Change:	950125	A2	Obligatory supplementary classification (change)
Examination:	950920	A2	Date of filing of request for examination: 950725
Examination:	951108	A2	Date of despatch of first examination report: 950921
Change:	971126	A2	Title of invention (English) (change)
Change:	971126	A2	Title of invention (French) (change)
Grant:	980909	B1	Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9837	658
CLAIMS B	(German)	9837	674
CLAIMS B	(French)	9837	802
SPEC B	(English)	9837	4235

Total word count - document A 0
Total word count - document B 6369
Total word count - documents A + B 6369

12/5/1
DIALOG(R)File 348:European Patents

00762159
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Security enclosure
Sicherheitszaun
Cloture de securite
PATENT ASSIGNEE:
W.L. GORE & ASSOCIATES, INC., (268452), 555 Paper Mill Road, P.O. Box 9206, Newark, Delaware 19714-9206, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
Macpherson, Hugh, 12 Balfour Crescent, Kinross KY13 7TA, (GB)
LEGAL REPRESENTATIVE:
Shanks, Andrew et al (74561), Cruikshank & Fairweather, 19 Royal Exchange Square, Glasgow G1 3AE, (GB)
PATENT (CC, No, Kind, Date): EP 715283 A1 960605 (Basic)
APPLICATION (CC, No, Date): EP 96101735 890614;
PRIORITY (CC, No, Date): GB 8814471 880617
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: G08B-013/12; G06F-001/00;

ABSTRACT EP 715283 A1
A security enclosure is formed from layers of flexible material. One layer (11;18) carries a flexible semiconductive line (10,13) arranged to extend over the whole area of the enclosure. Any interruption of the line by unauthorised opening of the enclosure changes the resistance of the line and so can be detected by a monitoring circuit. Further, two layers (17) of semiconductive fibres also cover the whole area of the enclosure and are separated by an insulating layer (16). The length of the fibres is greater than the thickness of the insulating layer (16) so that if the enclosure is pierced fibres from one layer (17) will be forced into contact with fibres from the other layer (17). This will change the combined resistance of the layers and this can also be detected by a monitoring circuit. The two measures can be used separately. (see image in original document)
ABSTRACT WORD COUNT: 171

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	960605 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	960605 A1	Date of filing of request for examination: 960220
Withdrawal:	970305 A1	Date on which the European patent application was withdrawn: 970102

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB96	1375
SPEC A	(English)	EPAB96	3987

Total word count - document A 5362
Total word count - document B 0
Total word count - documents A + B 5362

12/5/2
DIALOG(R)File 348:European Patents

00735078
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
IMAGE-RECEIVING ELEMENT FOR THERMAL DYE TRANSFER METHOD
BILDEMPFANGSELEMENT FUR THERMISCHES FARBSTOFFUBERTRAGUNGSVERFAHREN
ELEMENT RECEPTEUR D'IMAGE POUR UNE TECHNIQUE DE TRANSFERT THERMIQUE DE COLORANT
PATENT ASSIGNEE:
POLAROID CORPORATION, (200011), 549 Technology Square, Cambridge, Massachusetts 02139-3589, (US), (applicant designated states: CH;DE;FR;GB;IT;LI;NL;SE)
INVENTOR:
CHIANG, Yunn, H., 5 Bradley Road, Andover, MA 01810, (US)
GAUDIANA, Russell, A., 2 Penrose Lane, Merrimack, NH 03054, (US)
LEGAL REPRESENTATIVE:
Reitzner, Bruno, Dr. et al (9513), Patentanwalte Dipl.-Ing. R. Splanemann Dr. B. Reitzner, Dipl.-Ing. K. Baronetzky Tal 13, 80331 Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 756545 A1 970205 (Basic)
EP 756545 B1 980923
WO 9529066 951102
APPLICATION (CC, No, Date): EP 95905473 941220; WO 94US14952 941220
PRIORITY (CC, No, Date): US 231119 940422
DESIGNATED STATES: CH; DE; FR; GB; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: B41M-003/14; B42D-015/10; B32B-027/08;
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	960117 A	International application (Art. 158(1))
Application:	970205 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	970205 A1	Date of filing of request for examination: 961005
Examination:	970305 A1	Date of despatch of first examination report: 970122
Grant:	980923 B1	Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9839	523
CLAIMS B	(German)	9839	505
CLAIMS B	(French)	9839	739
SPEC B	(English)	9839	7491
Total word count - document A			0
Total word count - document B			9258
Total word count - documents A + B			9258

12/5/3
DIALOG(R)File 348:European Patents

00621918
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Security threads and security paper using the same
Sicherheitsfaden, und ihre Verwendung in Sicherheitspapier
Fils de securite, et papier de securite les utilisant
PATENT ASSIGNEE:
PORTALS (BATHFORD) LIMITED, (1738540), 6 Agar Street, London WC2N 4DE, (GB), (applicant designated states: DE;DK;ES;FR;IT;NL)
INVENTOR:
Jotcham, Richard Bryan, Silverlands, 12 Windsor Drive, Trowbridge, Wiltshire BA14 0JZ, (GB)
Payne, Gerald Sydney, 11 Northmead Close, Midsomer Norton, Bath, Avon BA3 2SG, (GB)
LEGAL REPRESENTATIVE:

Bucks, Teresa Anne et al (62861), BOULT WADE TENNANT, 27 Furnival Street, London EC4A 1PQ, (GB)
PATENT (CC, No, Kind, Date): EP 608078 A1 940727 (Basic)
EP 608078 B1 980715
APPLICATION (CC, No, Date): EP 94300264 940114;
PRIORITY (CC, No, Date): GB 9300998 930120
DESIGNATED STATES: DE; DK; ES; FR; IT; NL
INTERNATIONAL PATENT CLASS: D21H-021/48; D21H-021/42; B42D-015/00;

ABSTRACT EP 608078 A1
The specification discloses with reference to Figure 1, a security thread (11) for use in security articles (10), said thread (11) comprising a substrate having a coating on one or both sides of the substrate, said coating containing a thermochromic material selected from pigments and dyestuffs which material changes from coloured to colourless when the temperature of said pigment or dyestuff is changed to the activation temperature. The thermochromic material may be coloured when the temperature is below the activation temperature and becomes colourless when the material is at the activation temperature or above. The thread (11) is for security paper (10) for use in producing banknotes and the like.
ABSTRACT WORD COUNT: 112

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	940727	A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	940831	A1	Date of filing of request for examination: 940701
Examination:	951213	A1	Date of despatch of first examination report: 951026
Change:	960807	A1	Representative (change)
Change:	970319	A1	Designated Contracting States (change)
Grant:	980715	B1	Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9829	655
CLAIMS B	(German)	9829	639
CLAIMS B	(French)	9829	699
SPEC B	(English)	9829	3481
Total word count - document A			0
Total word count - document B			5474
Total word count - documents A + B			5474

12/5/4
DIALOG(R)File 348:European Patents

00540851
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Improvements in security enclosures
Sicherheitsbehalter
Recipient de securite
PATENT ASSIGNEE:
W.L. GORE & ASSOCIATES (UK) LTD, (1198130), 1 Bell Yard, London WC2A 2JP, (GB), (applicant designated states: DE;DK;ES;FR;GB;IT;SE)
INVENTOR:
MacPherson, Hugh, 12 Balfour Crescent, Milnathort, Fife, Scotland, (GB)
LEGAL REPRESENTATIVE:
MacDougall, Donald Carmichael et al (33372), Cruikshank & Fairweather 19 Royal Exchange Square, Glasgow G1 3AE, Scotland, (GB)
PATENT (CC, No, Kind, Date): EP 540139 A2 930505 (Basic)
EP 540139 A3 931006
EP 540139 B1 980909
APPLICATION (CC, No, Date): EP 92305198 920605;
PRIORITY (CC, No, Date): GB 9113455 910621

DESIGNATED STATES: DE; DK; ES; FR; GB; IT; SE
INTERNATIONAL PATENT CLASS: G08B-013/12;
CITED PATENTS (EP A): GB 1375926 A; GB 2220513 A

ABSTRACT EP 540139 A2

A security enclosure comprises a flexible sheet (60) of insulating material extending over the whole of the area of the enclosure and carrying lines (62, 64) of electrically-responsive material on each side. The lines on one side of the sheet (60) extend obliquely relative to the lines on the other side of the sheet and are connected thereto at edge portions of the sheet to form a plurality of conductors so dividing the sheet into a number of relatively small areas so that attempted opening of the enclosure changes an electrical characteristic of the conductors. Connectors (70) are provided at an edge portion of the sheet (60) for individually connecting the conductors to a detector (88) for detecting the changes in the electrical characteristic of the lines (62, 64). The connectors (70) include a switch arrangement which is selectively configured to connect further connectors (72) associated with the detector (88) with selected conductors. One edge portion of the sheet includes a plurality of line switches (66a - d) which are selectively configured to connect each one of the lines (62a - d) on one side of the sheet with a selected one of a plurality of lines (64a - d) on the other side of the sheet. (see image in original document)
ABSTRACT WORD COUNT: 214
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	930505	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	931006	A3	Separate publication of the European or International search report
Examination:	940518	A2	Date of filing of request for examination: 940318
Examination:	970528	A2	Date of despatch of first examination report: 970414
Grant:	980909	B1	Granted patent

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9837	1331
CLAIMS B	(German)	9837	1256
CLAIMS B	(French)	9837	1467
SPEC B	(English)	9837	5279
Total word count - document A			0
Total word count - document B			9333
Total word count - documents A + B			9333

12/5/5
DIALOG(R)File 348:European Patents

00447581
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
SECURITY DOCUMENT WITH EMBEDDED SECURITY ELEMENT WITH VISUALLY AND MECHANICALLY VERIFIABLE DISTINGUISHING SIGNS.
SICHERHEITSDOKUMENT MIT DARIN EINGEBETTETEM SICHERHEITSELEMENT MIT VISUELL UND MASCHINELL PRUFBAREN KENNZEICHEN.
PIECE D'IDENTITE COMPORTANT UN ELEMENT DE SECURITE ENCASTRE ET DES ELEMENTS D'IDENTIFICATION A VERIFICATION MECANIQUE.
PATENT ASSIGNEE:
GAO Gesellschaft fur Automation und Organisation mbH, (271480), Postfach 70 07 03, D-81307 Munchen, (DE), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
KAULE, Wittich, Lindacher Weg 13, D-8080 Emmering, (DE)
BOHM, Michael, Konigsbergerstr. 20, D-8015 Markt Schwaben, (DE)
LEGAL REPRESENTATIVE:
Klunker . Schmitt-Nilson . Hirsch (101001), Winzererstrasse 106, D-80797

Munchen, (DE)
PATENT (CC, No, Kind, Date): EP 426801 A1 910515 (Basic)
EP 426801 B1 950322
WO 9013877 901115
APPLICATION (CC, No, Date): EP 90906985 900511; WO 90EP765 900511
PRIORITY (CC, No, Date): DE 3915638 890512
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: G07D-007/00; G07F-007/08; B42D-015/02;
B42D-015/00; B44F-001/12; D21H-021/48;
CITED PATENTS (WO A): GB 500151 A; EP 279880 A; DE 1446851 A
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	910515 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	910515 A1	Date of filing of request for examination: 901217
Examination:	931215 A1	Date of despatch of first examination report: 931029
Grant:	950322 B1	Granted patent
Lapse:	960124 B1	Date of lapse of the European patent in a Contracting State: BE 950322
Oppn:	960221 B1	Opposition 01/951227 ARJO WIGGINS S.A.; 117 Quai du President Roosevelt; 92442 Issy-les-Moulineaux Cedex; (FR) (Representative:)Remy, Vincent Noel Paul (FR); Cabinet Nony & Associes 29, rue Cambaceres; F-75008 Paris; (FR)
Lapse:	961016 B1	Date of lapse of the European patent in a Contracting State: AT 950511, BE 950322
Oppn Ended:	970108 B1	Termination of opposition procedure: 960823

LANGUAGE (Publication,Procedural,Application): German; German; German
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPAB95	641
CLAIMS B	(German)	EPAB95	546
CLAIMS B	(French)	EPAB95	686
SPEC B	(German)	EPAB95	2527
Total word count - document A			0
Total word count - document B			4400
Total word count - documents A + B			4400

12/5/6
DIALOG(R)File 348:European Patents

00412272
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
IMAGING PLASTICS ARTICLES
BILDHERSTELLUNG AUF KUNSTSTOFFGEGENSTANDE
ARTICLES D'IMAGERIE EN MATIERE PLASTIQUE
PATENT ASSIGNEE:
De La Rue plc, (648143), 6 Agar Street, London WC2N 4DE, (GB), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;LU;NL;SE)
INVENTOR:
CAUDELL, Martin, John 3 Woodside Cottages, Warren Row Wargrave, Berkshire RG10 8QU, (GB)
ELDRED, James, Raymond 21 Hill Farm Road, Marlow Bottom Marlow, Buckinghamshire SL7 3LX, (GB)
EZRA, David, 59 Hurst Park Road Twyford, Berkshire RG10 0EZ, (GB)
LEGAL REPRESENTATIVE:
Skone James, Robert Edmund et al (50281), GILL JENNINGS & EVERY Broadgate House 7 Eldon Street, London EC2M 7LH, (GB)
PATENT (CC, No, Kind, Date): EP 444087 A1 910904 (Basic)
EP 444087 B1 971001
WO 9005640 900531
APPLICATION (CC, No, Date): EP 89912804 891117; WO 89GB1375 891117
PRIORITY (CC, No, Date): GB 8827062 881118; GB 8912664 890602

DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: B41M-001/30; B41M-005/26; B41M-003/14;
CITED PATENTS (WO A): US 4059471 A; US 2721821 A; CH 522510 A; EP 106663 A; EP 97528 A; EP 121323 A
CITED REFERENCES (EP A):
See also references of WO9005640;
CITED REFERENCES (WO A):
PATENT ABSTRACTS OF JAPAN, Vol. 11, No. 241 (M-614)(2688), 7 August 1987; & JP-A-6253887 (Ricoh Co. LTD) 9 March 1987
Product Licensing Index, No. 96, April 1972, Silk Screen Dyeing of Films with Disperse Dyes page 31* Abstract No. 9602*;
LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	910904	A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	910904	A1	Date of filing of request for examination: 910510
*Assignee:	920115	A1	Applicant (transfer of rights) (change): De La Rue plc (648142) De La Rue House, 3/5 Burlington Gardens London W1A 1DL (GB) (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;LU;NL;SE)
*Assignee:	920115	A1	Previous applicant in case of transfer of rights (change): THE DE LA RUE COMPANY PLC (648140) De La Rue House, 3/5 Burlington Gardens London W1A 1DL (GB) (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;LU;NL;SE)
*Assignee:	921104	A1	Applicant (transfer of rights) (change): De La Rue plc (648143) 6 Agar Street London WC2N 4DE (GB) (applicant designated states: AT;BE;CH;DE;ES;FR;GB;IT;LI;LU;NL;SE)
Examination:	951011	A1	Date of despatch of first examination report: 950823
Grant:	971001	B1	Granted patent
Lapse:	980520	B1	Date of lapse of the European patent in a Contracting State: SE 980101
Oppn None:	980923	B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	9709W4	728
CLAIMS B	(German)	9709W4	713
CLAIMS B	(French)	9709W4	792
SPEC B	(English)	9709W4	6852
Total word count - document A			0
Total word count - document B			9085
Total word count - documents A + B			9085

12/5/7
DIALOG(R)File 348:European Patents

00401503
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Security paper.
Sicherheitspapier.
Papier de securite.
PATENT ASSIGNEE:
PORTALS LIMITED, (470601), Overton Mill, Overton, Basingstoke, Hampshire RG25 3JG, (GB), (applicant designated states: CH;DE;DK;ES;FR;IT;LI;NL;SE)
INVENTOR:
Edwards, David John, 22 Lordsfield, Overton, Hampshire, (GB)
LEGAL REPRESENTATIVE:
Hardisty, David Robert et al (31501), BOULT, WADE & TENNANT 27 Furnival Street, London EC4A IPQ, (GB)

PATENT (CC, No, Kind, Date): EP 400902 A2 901205 (Basic)
EP 400902 A3 911211
EP 400902 B1 940420
APPLICATION (CC, No, Date): EP 90305679 900524;
PRIORITY (CC, No, Date): GB 8912750 890602
DESIGNATED STATES: CH; DE; DK; ES; FR; IT; LI; NL; SE
INTERNATIONAL PATENT CLASS: D21H-021/42; B41M-003/14;
CITED PATENTS (EP A): EP 319157 A; EP 319157 A; EP 70172 A; EP 70172 A; FR 2365657 A; FR 2365657 A; EP 59056 A; GB 1604463 A

ABSTRACT EP 400902 A2

This invention is concerned with security paper (3) for bank notes, cheques and like documents in a security strip of enhanced security which is more difficult to counterfeit than the present bank notes containing window threads. Security papers according to the invention comprise at least one elongated security element (4) which security element is partially embedded within said paper with portions thereof being exposed at the surface of the paper at spaced intervals along the length of the security element at windows in the paper, said security element being visually detectable in transmitted light and being visible in the windows of the paper in reflected light, wherein the said security element comprises a plurality of layers including a support layer (11) and metallic regions (12) such that when the exposed portions of the security element are viewed in reflected light there is visible to the unaided eye in each window at least two metallic areas (1, 2) which form repeating patterns along the length of the element, with the said metallic areas being of different colour.

ABSTRACT WORD COUNT: 180

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	901205	A2	Published application (A1with Search Report ;A2without Search Report)
Examination:	901205	A2	Date of filing of request for examination: 900601
Search Report:	911211	A3	Separate publication of the European or International search report
Change:	930310	A2	Designated Contracting States (change)
Examination:	930512	A2	Date of despatch of first examination report: 930324
Grant:	940420	B1	Granted patent
Oppn None:	950412	B1	No opposition filed
Lapse:	970423	B1	Date of lapse of the European patent in a Contracting State: SE 960525

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	747
CLAIMS B	(German)	EPBBF1	659
CLAIMS B	(French)	EPBBF1	823
SPEC B	(English)	EPBBF1	4827
Total word count - document A			0
Total word count - document B			7056
Total word count - documents A + B			7056

12/5/8

00366279

Security enclosure
Sicherheitszaun
Cloture de securite

PATENT ASSIGNEE:

W.L. GORE & ASSOCIATES, INC., (268452), 555 Paper Mill Road, P.O. Box 9206, Newark, Delaware 19714-9206, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;GR;IT;LI;LU;NL;SE)

INVENTOR:
MacPherson, Hugh, 12 Balfour Crescent, Milnathort Kinross-shire Scotland, (GB)
LEGAL REPRESENTATIVE:
McCallum, William Potter et al (33662), Cruikshank & Fairweather 19 Royal Exchange Square, Glasgow G1 3AE Scotland, (GB)
PATENT (CC, No, Kind, Date): EP 347209 A2 891220 (Basic)
EP 347209 A3 910717
EP 347209 B1 960918
APPLICATION (CC, No, Date): EP 89306035 890614;
PRIORITY (CC, No, Date): GB 8814471 880617
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: G08B-013/12;
CITED PATENTS (EP A): US 3594770 A; US 3594770 A; DE 3527873 A; FR 2411294 A; CH 525524 A; FR 2555783 A

ABSTRACT EP 347209 A2
A security enclosure is formed from layers of flexible material. One layer (11;18) carries a flexible semiconductive line (10,13) arranged to extend over the whole area of the enclosure. Any interruption of the line by unauthorised opening of the enclosure changes the resistance of the line and so can be detected by a monitoring circuit. Further, two layers (17) of semiconductive fibres also cover the whole area of the enclosure and are separated by an insulating layer (16). The length of the fibres is greater than the thickness of the insulating layer (16) so that if the enclosure is pierced fibres from one layer (17) will be forced into contact with fibres from the other layer (17). This will change the combined resistance of the layers and this can also be detected by a monitoring circuit. The two measures can be used separately.
ABSTRACT WORD COUNT: 147

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	891220 A2	Published application (A1with Search Report ;A2without Search Report)
Change:	901003 A2	Representative (change)
Search Report:	910717 A3	Separate publication of the European or International search report
Examination:	920122 A2	Date of filing of request for examination: 911125
Examination:	940622 A2	Date of despatch of first examination report: 940510
Change:	960918 A2	Miscellaneous (change)
Grant:	960918 B1	Granted patent
Oppn None:	970910 B1	No opposition filed

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1628
CLAIMS B	(English)	EPAB96	1413
CLAIMS B	(German)	EPAB96	1492
CLAIMS B	(French)	EPAB96	1553
SPEC A	(English)	EPABF1	3992
SPEC B	(English)	EPAB96	4036
Total word count - document A			5620
Total word count - document B			8494
Total word count - documents A + B			14114

12/5/9
DIALOG(R)File 348:European Patents

00318027
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
A security system and a signal-carrying member therefor.
Sicherheitssystem und ein signaltragendes Glied dafur.
Systeme de securite et un membre portant un signal a cet effet.

PATENT ASSIGNEE:
W.L. GORE & ASSOCIATES, INC., (268452), 555 Paper Mill Road P.O. Box 9206 , Newark Delaware 19714, (US), (applicant designated states: AT;BE;CH;DE;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
MacPherson, Hugh, 12, Balfour Crescent Milnathort, Kinross-shire Scotland , (GB)
LEGAL REPRESENTATIVE:
McCallum, William Potter et al (33662), Cruikshank & Fairweather 19 Royal Exchange Square, Glasgow G1 3AE Scotland, (GB)
PATENT (CC, No, Kind, Date): EP 317101 A2 890524 (Basic)
EP 317101 A3 890927
EP 317101 B1 931201
APPLICATION (CC, No, Date): EP 88310110 881027;
PRIORITY (CC, No, Date): GB 8727092 871119
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: H01B-007/32; G01R-031/02;
CITED PATENTS (EP A): EP 120479 A; EP 49104 A; GB 378634 A

ABSTRACT EP 317101 A2
A security system comprises a signal-carrying member and a detector for detecting a change in the resistance of a conductive path surrounding a core of the signal-carrying member. The conductive path comprises inner and outer layers (11,13) of semi-conductive tape separated by an insulating layer (12) but interconnected at one end. The semi-conductive tape of at least the outer layer is made of fibrous material such as carbon-loaded PTFE such that when a sharp object pierces the outer layer (13) and the insulating layer (12), semi-conductive fibres are dragged from the outer layer into contact with the inner layer (11) and form a conductive bridge between the layers.
ABSTRACT WORD COUNT: 112

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	890524	A2	Published application (Alwith Search Report ;A2without Search Report)
Search Report:	890927	A3	Separate publication of the European or International search report
Change:	890927	A2	Obligatory supplementary classification (change)
Examination:	900509	A2	Date of filing of request for examination: 900305
Change:	900822	A2	Representative (change)
Examination:	920624	A2	Date of despatch of first examination report: 920507
Grant:	931201	B1	Granted patent
Lapse:	940803	B1	Date of lapse of the European patent in a Contracting State: CH 931201, LI 931201
Lapse:	940803	B1	Date of lapse of the European patent in a Contracting State: CH 931201, LI 931201
Lapse:	940928	B1	Date of lapse of the European patent in a Contracting State: CH 931201, LI 931201, NL 931201
Lapse:	941117	B1	Date of lapse of the European patent in a Contracting State: AT 931201, CH 931201, LI 931201, NL 931201
Oppn None:	941123	B1	No opposition filed
Lapse:	941130	B1	Date of lapse of the European patent in a Contracting State: AT 931201, BE 931201, CH 931201, LI 931201, NL 931201

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	525
CLAIMS B	(German)	EPBBF1	537
CLAIMS B	(French)	EPBBF1	577
SPEC B	(English)	EPBBF1	2975

Total word count - document A 0

Total word count - document B 4614
Total word count - documents A + B 4614

12/5/10
DIALOG(R)File 348:European Patents

00305280
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Device for the protected storage of objects.
Vorrichtung zum geschutzten Aufbewahren von Sachen.
Dispositif pour l'entrepot protege d'objets.
PATENT ASSIGNEE:
Seculock B.V., (937870), Nieuwe Hescheweg 23, NL-5342 CE Oss, (NL),
(applicant designated states: AT;BE;CH;DE;ES;FR;GB;GR;IT;LI;LU;NL;SE)
INVENTOR:
Tel, Teunis, Gorterlaan 19, NL-9721 ZA Groningen, (NL)
LEGAL REPRESENTATIVE:
van der Arend, Adrianus G.A., Ir. et al , EXTERPATENT Willem Witsenplein 4, NL-2596 BK 's-Gravenhage, (NL)
PATENT (CC, No, Kind, Date): EP 277679 A1 880810 (Basic)
APPLICATION (CC, No, Date): EP 88200099 880120;
PRIORITY (CC, No, Date): NL 87165 870123
DESIGNATED STATES: AT; BE; CH; DE; ES; FR; GB; GR; IT; LI; LU; NL; SE
INTERNATIONAL PATENT CLASS: E05G-005/00;
CITED PATENTS (EP A): AU 426267 B; EP 190778 A; FR 2445429 A

ABSTRACT EP 277679 A1
Device for the protected storage of objects, comprising a closable container having an electrical security shield enclosing a storage space, damaging means (10) for rendering the objects useless, and means (4) for feeding in from the outside a command which disables the damaging means (10), the security shield comprising one or more electrical systems which at least together extend over essentially the entire surface of the shield and which cooperate with a processing circuit (14) which detects an electrical parameter of each system, and which is capable of delivering an activation command to the damaging means (10) when a detected parameter value deviates from a reference value.
ABSTRACT WORD COUNT: 111

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	880810 A1	Published application (A1with Search Report ;A2without Search Report)
Examination:	890329 A1	Date of filing of request for examination: 890130
Examination:	910502 A1	Date of despatch of first examination report: 910314
Withdrawal:	920401 A1	Date on which the European patent application was deemed to be withdrawn: 910925

LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPABF1	1152
SPEC A	(English)	EPABF1	3559
Total word count - document A			4711
Total word count - document B			0
Total word count - documents A + B			4711

12/5/11
DIALOG(R)File 348:European Patents

00265165
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
High-security identification card obtained by thermal dye transfer.

Hochsicherheits-Identifikationskarte, hergestellt durch thermische Farbubertragung.
Carte d'identite de haute securite, obtenue par transfert thermique de colorant.

PATENT ASSIGNEE:
EASTMAN KODAK COMPANY (a New Jersey corporation), (201210), 343 State Street, Rochester New York 14650, (US), (applicant designated states: BE;CH;DE;FR;GB;LI;NL)
INVENTOR:
Sethi, Gurdip S. c/o EASTMAN KODAK COMPANY, Patent Department 343 State Street, Rochester New York 14650, (US)
Marshall, Stephen D. c/o EASTMAN KODAK COMPANY, Patent Department 343 State Street, Rochester New York 14650, (US)
Wenschhof, David E. c/o EASTMAN KODAK COMPANY, Patent Department 343 State Street, Rochester New York 14650, (US)
LEGAL REPRESENTATIVE:
Brandes, Jurgen, Dr.Rer.Nat. et al (2381), Wuesthoff & Wuesthoff Patent- und Rechtsanwalte Schweigerstrasse 2, D-8000 Munchen 90, (DE)
PATENT (CC, No, Kind, Date): EP 273348 A2 880706 (Basic)
EP 273348 A3 890329
EP 273348 B1 901122
APPLICATION (CC, No, Date): EP 87118945 871221;
PRIORITY (CC, No, Date): US 947052 861229
DESIGNATED STATES: BE; CH; DE; FR; GB; LI; NL
INTERNATIONAL PATENT CLASS: B42D-015/10; B41M-005/035;
CITED PATENTS (EP A): US 4629215 A; EP 149542 A; GB 2132136 A; GB 2120169 A

ABSTRACT EP 273348 A2

A dye-receiving element and process for producing a high-security, monolithic identification card, the element comprising a support having thereon a dye image-receiving layer adapted to receive a thermally-transferred dye image, the dye image-receiving layer containing indicia printed thereon having a linewidth of approximately 40-120 (mu)m.

ABSTRACT WORD COUNT: 49

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	880706	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	890329	A3	Separate publication of the European or International search report
Examination:	890705	A2	Date of filing of request for examination: 890428
*Assignee:	890830	A2	Applicant (transfer of rights) (change): EASTMAN KODAK COMPANY (a New Jersey corporation) (201210) 343 State Street Rochester New York 14650 (US) (applicant designated states: BE;CH;DE;FR;GB;LI;NL)
Examination:	900103	A2	Date of despatch of first examination report: 891120
Change:	900207	A2	Representative (change)
Grant:	901122	B1	Granted patent
Oppn:	911009	B1	Opposition 01/910816 Thomas De La Rue & Company Ltd.; 3/5 Burlington Gardens; London W1A 1DL; (GB) (Representative:)Skone James, Robert Edmund; GILL JENNINGS & EVERY 53-64 Chancery Lane; London WC2A 1HN; (GB)
Oppn:	911016	B1	Opposition 01/910816 Thomas De La Rue & Company Ltd.; 3/5 Burlington Gardens; London W1A 1DL; (GB) (Representative:)Skone James, Robert Edmund; GILL JENNINGS & EVERY 53-64 Chancery Lane; London WC2A 1HN; (GB) 02/910821 GAO Gesellschaft fur Automation und Organisation mbH; Euckenstrasse 12; W-8000 Munchen 70; (DE)

*Oppn: 920819 B1 Opposition (change) 01/910816 Thomas De La Rue & Company Ltd.; 3/5 Burlington Gardens; London W1A 1DL; (GB)
(Representative:)Skone James, Robert Edmund; GILL JENNINGS & EVERY 53-64 Chancery Lane; London WC2A 1HN; (GB)
02/910821 GAO Gesellschaft fur Automation und Organisation mbH; Euckenstrasse 12; W-8000 Munchen 70; (DE)
(Representative:)Klunker, Hans-Friedrich, Dr.; Patentanwalte Klunker . Schmitt-Nilson . Hirsch Winzererstrasse 106; W-8000 Munchen 40; (DE)
Revocation: 950816 B1 Revocation of the European patent: 950331
Lapse: 951206 B1 Date of lapse of the European patent in a Contracting State: CH 901122, LI 901122
Lapse: 951206 B1 Date of lapse of the European patent in a Contracting State: CH 901122, LI 901122
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPABF1	322
SPEC B	(English)	EPABF1	2871
Total word count - document A			0
Total word count - document B			3193
Total word count - documents A + B			3193

12/5/12
DIALOG(R)File 348:European Patents

00224466
ORDER fax of complete patent from Dialog SourceOne. See HELP ORDER 348
Communications network.
Kommunikationsnetz.
Reseau de communication.
PATENT ASSIGNEE:
THORN EMI Electronics Limited, (716110), Blyth Road, Hayes Middlesex UB3 1DL, (GB), (applicant designated states: DE;FR;GB)
INVENTOR:
Marzolini, Remo Giovanni Andrea, 16, Hibernia Gardens, Hounslow Middlesex, TW3 3SD, (GB)
LEGAL REPRESENTATIVE:
Hurst, Richard Arthur Alexander et al (32172), THORN EMI Patents Limited, Central Research Laboratories, Dawley Road, Hayes, Middlesex UB3 1HH, (GB)
PATENT (CC, No, Kind, Date): EP 228830 A2 870715 (Basic)
EP 228830 A3 890215
EP 228830 B1 921028
APPLICATION (CC, No, Date): EP 86309490 861205;
PRIORITY (CC, No, Date): GB 8531209 851218
DESIGNATED STATES: DE; FR; GB
INTERNATIONAL PATENT CLASS: H04L-009/00;
CITED PATENTS (EP A): EP 69831 A
CITED REFERENCES (EP A):
ELECTRONICS INTERNATIONAL, vol. 53, no. 25, November 1980, pages 76,77, New York, US; J. GOSCH: "Portable case holds cryptographic unit"
TELECOM REPORT, vol. 1, no. 3, June 1978, pages 160-163, Munich, DE; F. STR SSER: "Fernschreiber 1000 CA, eine Investition f}r die Sicherheit";

ABSTRACT EP 228830 A2
Transmitter station 1 has a data source, a crypto unit 4, a buffer store 5 for encrypted signals and a transmitter 6 with an aerial 7, all with a common power supply 8. A switching control unit 9 has a position in which it connects data source 3 and crypto unit 4 to the power supply 8 but isolates transmitter 6 therefrom, and another switch position in which transmitter 6 is connected to the power supply 8 while data source

3 and crypto unit 4 are isolated therefrom. In this way, if any signals output from data source 3 pass directly (i.e. not via crypto unit 4) to the input of transmitter 6, they will not be sent on into the network because transmitter 6 is "off" (i.e. de-energised) at that time.

ABSTRACT WORD COUNT: 136

LEGAL STATUS (Type, Pub Date, Kind, Text):

Application:	870715	A2	Published application (A1with Search Report ;A2without Search Report)
Search Report:	890215	A3	Separate publication of the European or International search report
Examination:	890726	A2	Date of filing of request for examination: 890524
Examination:	910703	A2	Date of despatch of first examination report: 910521
Change:	911002	A2	Representative (change)
Grant:	921028	B1	Granted patent
Oppn None:	931020	B1	No opposition filed
Lapse:	940112	B1	Date of lapse of the European patent in a Contracting State: GB 930128

LANGUAGE (Publication,Procedural,Application): English; English; English

FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS B	(English)	EPBBF1	308
CLAIMS B	(German)	EPBBF1	386
CLAIMS B	(French)	EPBBF1	486
SPEC B	(English)	EPBBF1	2201
Total word count - document A			0
Total word count - document B			3381
Total word count - documents A + B			3381

?

java same stream same (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher)

(java near5 stream and (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher)) not (java near2 stream and (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher))

java near5 stream and (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher)

java near2 stream and (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher)

java near2 stream

java adj1 stream

java adj1 stream and (encrypt$3 or decrypt$3 or dec$1pher or enc$1pher)

java adj1 stream same encrypt$3

java adj1 stream same decrypt$3

application adj1 layer near5 (encrypt$3 or decrypt$3)

(layer or protocol) same (encrypt$3 or decrypt$3) same data adj1 stream

(layer or protocol) same (encrypt$3 or decrypt$3) same stream

((layer or protocol) near2 independent same (encrypt$3 or decrypt$3)) not ((layer or protocol) adj1 independent same (encrypt$3 or decrypt$3))

(layer or protocol) near2 independent same (encrypt$3 or decrypt$3)

(layer or protocol) adj1 independent same (encrypt$3 or decrypt$3)

(layer or protocol) adj1 independent near5 (encrypt$3 or decrypt$3)

java same (encrypt$3 or decrypt$3) and data adj1 stream

java same (encrypt$3 or decrypt$3) and stream

java same (encrypt$3 or decrypt$3)

java same (encrypt$3 or decrypt$3) same stream

java same encryption same stream